МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ “ЖИТОМИРСЬКА ПОЛІТЕХНІКА”

Кваліфікаційна наукова
праця на правах рукопису

ДМИТРЕНКО ІГОР АНАТОЛІЙОВИЧ

УДК: 351.88;343.35

ДИСЕРТАЦІЯ
ДЕРЖАВНЕ УПРАВЛІННЯ ЦИФРОВОЮ ТРАНСФОРМАЦІЄЮ СИСТЕМИ ОХОРОНИ ЗДОРОВ’Я

Спеціальність 25.00.02 – механізми державного управління
Галузь знань – державне управління

Подається на здобуття наукового ступеня
доктора наук з державного управління

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ І.А. Дмитренко

Науковий консультант
Грицишен Димитрій Олександрович,
професор, доктор економічних наук,
доктор наук з державного управління,

Житомир – 2026

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 впливає 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 полягає в сукупності змін до нормативно-правових актів, адаптованих до Регламентів Європейського Союзу, 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).

Запропоновано 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;

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) 2017/746 (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.

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 Economica*s. 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: 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: 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: 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: 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: 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 Міжн. наук.-практ. конференції* (11-12 грудня 2025 р., Житомир). Житомир, 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 наук.-практ. Семінару* (9–10 жовтня 2025 р.., Житомир). Житомир, 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 наук.-практ. конференції з міжнародною участю* (12-13 грудня 2024 р., Житомир). Житомир, 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 наук.-практ. конференції* (7-8 грудня 2023 р., Житомир). Житомир, 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, 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, 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, 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 Всеукр. наук.-практ. семінару (6 жовтня 2023 р., Житомир). Житомир, 2023. С. 255-256.

33. Дмитренко І. Цифрова трансформація системи охорони здоров'я Європейським Союзом. Правова політика України: історія та сучасність: матеріали V Всеукр. наук.-практ. семінару (10 жовтня 2024 р., Житомир). Житомир, 2024. С. 232-234.

ЗМІСТ

ВСТУП…… 18

РОЗДІЛ 1. ТЕОРЕТИЧНІ ПОЛОЖЕННЯ ДЕРЖАВНОГО УПРАВЛІННЯ ЦИФРОВОЮ ТРАНСФОРМАЦІЄЮ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я …… 31

1.1. Передумови та фактори розвитку цифрової трансформації системи охорони здоров'я як об'єкту державного управління ……... 31

1.2. Джерельна база наукового дослідження державного управління цифровою трансформацією системи охорони здоров'я ……... 51

1.3. Понятійно-категоріальний апарат державного управління цифровою трансформацією системи охорони здоров'я ……..…… 71

Висновки до 1-го розділу ……. 86

РОЗДІЛ 2. МЕТОДОЛОГІЯ ДЕРЖАВНОГО УПРАВЛІННЯ ЦИФРОВОЮ ТРАНСФОРМАЦІЄЮ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я ……... 90

2.1. Вплив цифрової трансформації на властивості системи охорони здоров'я та процес прийняття державно-управлінських рішень …… 90

2.2. Принципи державного управління цифровою трансформацією системи охорони здоров'я …… 111

2.3. Методологічні положення державного управління цифровою трансформацією системи охорони здоров'я …… 135

Висновки до 2-го розділу ……. 155

РОЗДІЛ 3. СУЧАСНИЙ СТАН ТА НАСЛІДКИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я ЯК ОБ'ЄКТУ ДЕРЖАВНОГО УПРАВЛІННЯ ……..…… 159

3.1. Світові тенденції цифрової трансформації системи охорони здоров'я ……. 159

3.2. Сучасний стан та тенденції цифрової трансформації систем охорони здоров'я європейських країн …… 189

3.3. Сучасний стан та основні напрями цифрової трансформації системи охорони здоров'я України ……. 212
Висновки до 3-го розділу ……..…… 231

РОЗДІЛ 4. ЄВРОІНТЕГРАЦІЙНІ ІМПЕРАТИВИ ДЕРЖАВНОГО УПРАВЛІННЯ ПРОЦЕСАМИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ 234
4.1. Вимоги Європейського Союзу до цифрової трансформації системи охорони здоров’я …… 234
4.2. Регулювання безпеки процесу цифрової трансформації системи охорони здоров’я в Європейському Союзі …… 266
4.3. Особливості державного управління цифровою трансформацією в країнах-членах Європейського Союзу ……... 286
Висновки до 4-го розділу ……. 304

РОЗДІЛ 5. УДОСКОНАЛЕННЯ МЕХАНІЗМІВ ДЕРЖАВНОГО УПРАВЛІННЯ ПРОЦЕСАМИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СИСТЕМИ ОХОРОНИ ЗДОРОВ’Я …… 308
5.1. Механізм адаптації державного управління цифровою трансформацією системи охорони здоров’я до вимог Європейського Союзу …… 308
5.2. Державне регулювання використання технологій штучного інтелекту у функціонуванні системи охорони здоров’я …… 332
5.3. Механізми розширення інституційної спроможності державного управління цифровою трансформацією системи охорони здоров’я ….. 357
Висновки до 5-го розділу ……. 373
ВИСНОВКИ ……... 378
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ……... 387
ДОДАТКИ ……... 396

ВСТУП

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 в світі прикута увага політиків, вчених, бізнесу, користувачів, що обумовлено 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, із 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%.

[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).

- *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 підписані декларації з сімейними лікарями[5]). Проте залишається невирішеною сукупність проблем, що пов'язані із правовим регулюванням, 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.

---

[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).

[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).

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), Бастіан Гаук (Bastian Hauck), Мішель Пенже (Michel Pinget), Майк Ліпс (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 невирішеними залишаються сукупність проблем теоретичного та методологічного характеру: 1) питання структури та змістовного наповнення передумов і факторів розвитку цифрової трансформації системи охорони здоров'я як об'єкту 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 ЄС до цифрової трансформації системи охорони здоров'я;

- оцінити вимоги Європейського Союзу 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 ШІ 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) 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 ґрунтується 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 в 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 і 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 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;

- 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-економічна 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 громадянського 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);

- методологічні положення державного управління цифровою трансформацією системи охорони здоров’я, що сформовані зважаючи на 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 і 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 Європейському Союзі, 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 Європеського Союзу (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 як стратегічної складової;

- 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 пokоження 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 9 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 включені 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.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ПОЛОЖЕННЯ ДЕРЖАВНОГО УПРАВЛІННЯ ЦИФРОВОЮ ТРАНСФОРМАЦІЄЮ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я

1.1. Передумови та фактори розвитку цифрової трансформації системи охорони здоров'я як об'єкту державного управління

Цифрова трансформація системи охорони здоров'я є складним динамічним, мінливим об'єктом державного управління, що поєднує в собі елементи медико-біологічних, техніко-технологічних, політико-правових, соціально-економічних, міжнародно-безпекових систем та відносин. Безумовно, що цифрова трансформація системи охорони здоров'я є безповоротним, стратегічно важливим процесом, який має бути керованим, врегульованим та відповідати запитам стейкхолдерів. Цифрова трансформація значно розширює коло стейкхолдерів системи охорони здоров'я, що знову ж таки вимагає врахування їх запитів при реалізації державно-управлінських рішень. Все це є передумовами та визначальними факторами впливу на процеси цифрової трансформації та функціонування цифрової системи охорони здоров'я. Ідентифікація факторів розвитку цифрової трансформації системи охорони здоров'я дозволить визначити передумови розвитку методологічних та організаційних положень державного управління та розширити теоретичне знання про об'єкт державного управління та його модифікацію в умовах інформаційного суспільства.

Питання ключових напрямів реформування системи охорони здоров'я представлені в працях вітчизняних вчених: 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. Питання цифрової трансформації системи охорони здоров'я викладені в дослідженнях зарубіжних вчених, зокрема: Adler-Milstein J., Jha A.K., Agbo C.C., Mahmoud Q.H., Eklund J.M., Ashley E.A., Biancone P., Secinaro S., Marseglia R., Calandra D., Buntin M.B., Burke M.F., Hoaglin M.C., Blumenthal D., Char D.S., Shah N.H., Magnus D., Cresswell K.M., Worth A., Sheikh A., Dal Mas F., Massaro M., Rippa P., Secundo G., Dorsey E.R., Topol E.J., Free C., Phillips G., Watson L., Galli L., Felix L., Edwards P., Patel V., Haines A., Hsiao C.J., Hing E., Ashman J., Islam S.M.R., Kwak D., Kabir M.H., Hossain M., Kwak K.S., Koonin L.M., Hoots B., Tsang C.A., Leroy Z., Farris K., Jolly B., Antall P., McCabe B., Zelis C.B., Tong I., Harris A.M., Kruse C.S., Frederick B., Jacobson T., Monticone D.K., Kvedar J., Coye M. J., Everett W., Massaro M., Meskó B., Drobni Z., Bényei É., Gergely B., Győrffy Z., Raghupathi W., Raghupathi V., Raimo N., De Turi I., Albergo F., Vitolla F., Schallmo D., Williams C.A., Boardman L., Sims S., Reed J.E., Weaver T., Stoumpos A.I., Kitsios F., Talias M.A. та інші.

Іртищева І.О., Сергійчук С.І., Рябець Д.М. виділяють сукупність проблем та викликів, що пов'язані із цифровою трансформацією системи охорони здоров'я:

- діджиталізація на національному рівні не можлива без загальної і єдиної для всіх системи «eHealth» та нормативно-правової бази, яка робить її законною;

- необхідна розробка «Національної стратегії розвитку eHealth» з технічним завданням для її впровадження та актуалізацією «Плану заходів щодо розвитку електронної системи охорони здоров'я (ЕСОЗ)»;

- потрібна стандартизація, термінологія, базові довідники та упорядкована робота держреєстрів (компоненти, що дозволять «спілкуватися» однією мовою всім учасникам і обмінюватися даними);

- забезпечення технічних можливостей для медичних закладів, захист персональних даних пацієнтів і лікарів та збереження їх окремо від медичних даних;

- уніфікованого рішення щодо питання інфраструктури (інтернет, комп'ютери, мережева інфраструктура) та типові конфігурації для лікарень. Потрібен план інформатизації, виділення коштів обласного бюджету на закупівлю комп'ютерної техніки та оснащення закладів охорони здоров'я;

- необхідні фахівці, які будуть впроваджувати і супроводжувати eHealth, тому лікарні повинні співпрацювати з експертами та ІТ-компаніями для технічного супроводу, а для медичних працівників необхідно створити можливості для набуття необхідних цифрових компетенцій. За різними оцінками, в Україні більше половини медичних працівників вважають себе недостатньо обізнаними в комп'ютерних технологіях;

- вільний доступ до Інтернету усіх верств населення, що дозволить мати доступ до особистої медичної інформації, до інформації про заклад, лікаря, виписані рецепти, відпущені ліки, напрямки на дослідження та їх результати, до спільнот з певним станом здоров'я, до запису на прийом в режимі онлайн;

- система eHealth повинна бути сфокусована на людині, яка зможе управляти своїм здоров'ям, відслідковуючи призначення лікаря, отримуючи дистанційну підтримку лікаря-консультанта; зможе стати учасником процесу

надання медичних послуг, що включає використання дистанційних пристроїв моніторингу, фіксування симптомів в електронній формі, взаємодію з лікарем або командою управління захворюванням; а також зможе отримувати інформацію про профілактичні заходи для себе та своєї родини» [18].

Зазначені положення обумовлені сукупністюЗазначені факторів, які впливають як власне на саму систему охорони здоров'я, так і на процеси цифрової трансформації. Вихідні положення в цілому та мета і завдання державного управління цифровою трансформацією будуть залежні від сукупності факторів, які пропонуємо визначати наступним чином (табл. 1.1).

Характеризуючи суспільні фактори, варто наголосити на важливості їх врахування при формуванні механізмів державного управління цифровою трансформацією, адже цифровізація – це довгостроковий багатоетапний процес, а тому варто визначати пріоритети на кожному етапі. Відповідно до зазначеного суспільні фактори характеризуються наступним чином:

- соціальні фактори – це 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. Соціальні фактори характеризують наступні поняття: спосіб життя, стрес, шкідливі звички, ізоляція. Адже саме вони впливають на стан здоров'я людини і як наслідок визначають рівень громадського здоров'я населення країни. Це призводить до перевантаження системи охорони здоров'я хронічними пацієнтами через незмінність їхньої поведінки, а тому визначає потребу в цифровізації як процесів лікування хронічних хвороб, так і процесів профілактики та пропаганди здорового способу життя через цифрові інструменти.

Таблиця 1.1

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 ОБУМОВЛЕНІ 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 хвороб</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 ОБУМОВЛЕНІ 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>
</table>

Продовження таблиці 1.1

<table>
<tr><td colspan="3">РЕСУРСНІ ФАКТОРИ</td></tr>
<tr><td>Фінансові</td><td colspan="2">Кадрові</td></tr>
<tr><td>- 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 colspan="2">- сукупність кількісних і якісних характеристик кадрового потенціалу системи охорони здоров'я (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>
<tr><td>Інфраструктурні</td><td colspan="2">Техніко-технологічні</td></tr>
<tr><td>- 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</td><td colspan="2">- 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</td></tr>
<tr><td colspan="3">ДЕРЖАВНО-УПРАВЛІНСЬКІ ФАКТОРИ</td></tr>
<tr><td>Інституційні</td><td>Організаційні</td><td>Інформаційні</td></tr>
<tr><td>- 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</td><td>- 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</td><td>- 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</td></tr>
</table>

Продовження таблиці 1.1

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

- медичні - 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 хвороб. Стан здоров’я населення країни є одним з найбільш важливих факторів, що визначають пріоритети цифрової трансформації, адже вони впливають саме на медичну складову цифровізації, а саме цифровізацію медичних послуг в цілому та таких її складових як профілактика, консультування, лікування, діагностування, реабілітація та супровід.

- демографічні - 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. Демографічні фактори характеризуються старінням нації, депопуляцією та міграційними хвилями, а в умовах сьогодення, ще вимушеною внутрішньою міграцією через бойові дії. Це призводить до збільшення частки старого населення, що призводить до збільшення навантаження на систему охорони здоров’я, та територіальних дисбалансів, що впливає на структуру системи охорони здоров’я. Так, держава фізично не може побудувати нову лікарню в кожному селі або приставити до кожного літнього громадянина окремого медика. «Трансформаційні зміни у галузі охорони здоров’я та необхідність вирішення завдань щодо забезпечення належного рівня здоров’я населення в умовах обмежених часових і фінансових ресурсів та зростання очікувань споживачів медичної допомоги, обумовлює потребу у розробці та використанні новітніх інструментів у зазначеній сфері. Цифрові технології містять потенціал вирішувати складні завдання в охороні здоров’я шляхом впровадження інноваційних рішень, які полегшують доступ

до медичних послуг, оптимізують процеси діагностики та лікування, покращують комунікацію між пацієнтами і медичним персоналом, забезпечують більш ефективне управління системою охорони здоров’я. Без інноваційних рішень неможливо покращити демографічні показники та зменшити відставання щодо рівня здоров’я населення від середньосвітових стандартів» [9]. Цифровізація стає єдиним управлінським виходом для забезпечення екстериторіальності медичної допомоги; впровадження телемедицини та мобільних бригад; реалізація технологій цифрового моніторингу. Відповідно при запровадженні цифрових технологій варто враховувати вирішення таких завдань як забезпечення доступності, територіальної незалежності та зменшення навантаження.

- економічні - 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 рівня громадського здоров'я та змушує прискорювати цифровізацію системи охорони здоров’я. Негативний вплив економічних факторів (економічні кризи, інфляція, безробіття) зумовлений рівнем бідності населення, неякісним харчуванням, відмовою від профілактики, запущеними станами. Це призводить до стрімкого падіння рівня громадського здоров’я, адже економічні фактори є фінансовим обмежувачем. Цифрова трансформація системи охорони здоров’я може зневолювати сукупність економічних факторів не стільки в частині здешевленняв частині медичної послуги, скільки в зменшенні супутніх витрат (витрати часу (зокрема робочого) для отримання консультації; витрати на проживання; витрати на проїзд та інші).

Підводячи підсумок характеристики суспільних факторів, можна зазначити, що державне управління цифровою трансформацією системи охорони здоров’я це не про технічне оновлення, а про інструменти

оптимізації, зниження соціальної напруги та зменшення завантаженості на систему охорони здоров’я. Крім того, цифровізація дозволяє державі приймати ефективні державно-управлінські рішення з обмеженими ресурсами в умовах, коли населення потребує більше медичної допомоги.

Цифрова трансформація, окрім вирішення сукупності суспільних проблем породжує сукупність викликів, а саме протидія соціальному супротиву, через низьку цифрову компетентність населення (особливо населення похилого віку); неготовність кадрового потенціалу до впровадження сучасних технологій та потреба постійного навчання як в контексті медичних знань, так і в контексті технологічних знань; відсутність довіри до інформаційних технологій та відсутність етичних положень використання технологій штучного інтелекту.

Політико-правові фактори є вкрай важливими з позиції спроможності політичної влади реалізувати цифрову трансформацію системи охорони здоров’я, яка б відповідала євроінтеграційним процесам та формувала правове поле для забезпечення розвитку. До даних факторів пропонуємо відносити:

- правові фактори - 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. Розвиток технологій та поява нових цифрових інструментів в сфері реалізації медичних та суміжних послуг створюють правовий вакуум. Відсутність чітких правил призводить до ризиків порушення лікарської таємниці, юридичної незахищеності як лікаря, так і пацієнта. Це означає, що цифрова трансформація системи охорони здоров’я вимагає реформування законодавства в медичній сфері, адже вимагає закріплення та легалізації цифрових практик, використання технологій штучного інтелекту, інструментів телемедицини. «Інструменти

автоматизації, штучного інтелекту, Big Data та блокчейну відкривають можливості для переходу до проактивної, персоналізованої, аналітично обґрунтованої моделі надання допомоги. Проте їхня ефективність залежить не лише від технічної реалізації, а й від здатності забезпечити прозорість, етичність і захист прав громадян. Упровадження таких технологій має супроводжуватись не лише нормативним і технічним регулюванням, а й підготовкою кадрів нової генерації – аналітиків, цифрових фасилітаторів, консультантів з інклюзії» [66].

Це все спричиняє зміни правового поля взаємодії між суб'єктами системи охорони здоров'я в цілому та між пацієнтом і лікарем зокрема. Коли правовий імператив набирає чинності, він повністю переформатовує діяльність усіх медичних закладів. Накази Міністерства охорони здоров'я та постанови уряду трансформують діяльність закладів охорони здоров'я та суб'єктів державного управління охороною здоров'я. Правові фактори, окрім легалізації та врегулювання використання цифрових технологій в системі охорони здоров'я також можуть визначати напрями стимулювання до прискорення цифрової трансформації, зокрема: а) правова заборона аналогових дублікатів через скасування вимоги збереження паперових аналогів; б) нормативний примус до сумісності через законодавчу заборону сертифікації та фінансування медичних програм, які не здатні обмінюватися даними з центральною державною базою; в) законодавче закріплення правил відповідальності за телемедичні консультації та використання технологій штучного інтелекту.

- політичні фактори характеризують рівень політичної підтримки цифрової трансформації, стратегічну наступність державної політики, стабільність реалізації реформ та політичну готовність до довгострокового розвитку цифрової системи охорони здоров'я. Цифрова трансформація є довготривалим процесом, який зазвичай триває довше, ніж один

електоральний цикл (каденція парламенту чи президента), відповідно політичний фактор визначає чи готові змінні політичні еліти підтримувати та продовжувати реформу цифрової трансформації системи охорони здоров’я. Позитивний або негативний вплив політичних факторів визначається політичною волею (готовність суб’єктів законодавчої та виконавчої державної влади визначати цифрову трансформацію системи охорони здоров'я одним із пріоритетів державної політики); політична стабільність (забезпечення послідовності та безперервності реалізації державної політики цифрової трансформації незалежно від змін політичних еліт); політична підтримка (рівень підтримки цифрової трансформації з боку парламенту, уряду, політичних інститутів та інших суб'єктів формування та реалізації державної політики); стратегічна пріоритетність цифрової трансформації (включення цифрової трансформації охорони здоров’я до системи стратегічних пріоритетів державного розвитку); політична узгодженість (узгодженість цілей цифрової трансформації між різними суб’єктами державної політики та відсутність політичних суперечностей щодо напрямів її реалізації).

- міжнародні (євроінтеграційні) - визначають необхідність гармонізації цифрової трансформації системи охорони здоров’я з політикою Європейського Союзу, інтеграції до європейського цифрового медичного простору та впровадження європейських стандартів. Фактично характеризують сукупність зовнішніх чинників міжнародного середовища, що визначають напрями, умови та темпи цифрової трансформації системи охорони здоров'я шляхом формування міжнародних стандартів, інтеграційних процесів, міжнародного співробітництва та трансферу цифрових технологій. Під впливом міжнародного фактора національна медицина виходить за рамки локальних інтересів. Міжнародні фактори характеризуються наступними категоріями: євроінтеграційні процеси (гармонізація національної цифрової системи охорони здоров’я з

європейськими законодавством для інтеграції національної системи охорони здоров’я в європейський медичний простір); міжнародні стандарти (впровадження міжнародних стандартів щодо електронної охорони здоров'я, управління медичними даними, інтероперабельності, кібербезпеки та застосування технологій штучного інтелекту); міжнародне співробітництво (розвиток партнерства з міжнародними організаціями, іноземними державами, науковими установами та міжнародними проєктами у сфері цифрової охорони здоров'я); міжнародна технічна та фінансова підтримка (залучення міжнародної фінансової допомоги, грантових програм, інвестицій і технічної експертизи для розвитку цифрової системи охорони здоров’я); трансфер цифрових технологій (запозичення та адаптація міжнародного досвіду, цифрових платформ, інноваційних технологій і найкращих практик цифрової трансформації).

Політико-правові фактори задають системі імпульс і визначають інтенсивність цифрової трансформації системи охорони здоров’я та визначають правове поле даного процесу у відповідності до міжнародних вимог. Разом з тим вони формують цілісну систему прийняття державно-управлінських рішень щодо реалізації процесів цифрової трансформації системи охорони здоров’я. Відповідно успішна цифрова трансформація системи охорони здоров’я визначається синергетичним впливом правових, політичних та міжнародних факторів, які в сукупності формують каркас державного управління реформою.

Ресурсні фактори є матеріально-ресурсною основою запровадження реформ, яка визначає спроможність держави реалізувати задекларовані цілі щодо цифрової трансформації системи охорони здоров’я,

- фінансові - 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. Фінансові фактори визначають ліміти реалізації реформи. Якщо політична воля декларує тотальну цифровізацію, саме фінансовий фактор визначає, чи отримають заклади охорони здоров’я фінансові ресурси для закупівлі обладнання, програмного забезпечення та ліцензій. Державне фінансування має покривати як етап формування та впровадження механізмів цифрової трансформації системи охорони здоров’я на усіх рівнях управління та реалізації медичних послуг так і забезпечення довгострокового, безперебійного та безпечного функціонування цифрової системи охорони здоров’я.

- кадрові - сукупність кількісних і якісних характеристик кадрового потенціалу системи охорони здоров'я (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. Для нівелювання зазначених факторів, а точніше їх використання для прискорення процесів адаптації держава має забезпечити управління зазначеними факторами через впровадження обов’язкових професійних стандартів цифрової компетентності для медичних та управлінських кадрів, інтеграції ІТ-дисциплін у програми вищої медичної освіти та інтернатури, створення системи безперервного професійного розвитку з нарахуванням курсів з питань цифрової системи охорони здоров’я. Крім того, вагоме значення при управлінні кадровими факторами є формування положень, які стосуються методів використання технологій штучного інтелекту та етичних питань даних методів. Адже технології штучного інтелекту в професійній діяльності медичного персоналу все частіше займають найбільш вагому роль для діагностування та встановлення методів лікування.

- інфраструктурні - 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. Інфраструктура створює фізичний базис реформи, де ключовим критерієм є безперервність. На сьогодні є вкрай важливим забезпечення безпеки інфраструктури з одного боку та її використання для безпеки медичних послуг, медичного персоналу та пацієнтів. Ключовими інфраструктурними факторами є: рівень покриття широкосмуговим інтернетом віддалених територій; будівництво та функціонування державних захищених центрів обробки даних; забезпечення лікарень резервними джерелами живлення; рівень координації роботи з операторами зв'язку.

- техніко-технологічні - 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. «У сфері охорони здоров’я ключову роль відіграють системні підходи до впровадження єдиної техніко-технологічної платформи, яка має коректно працювати в усій галузі. Основою для таких системних рішень є розуміння того, що завдання для закладів охорони здоров’я з питань трансформаційних змін галузі мають бути вимірюваними та досяжними, а використовувані новітні технології відповідати світовим стандартам» [9]. Даний фактор встановлює функціональні можливості цифрової трансформації системи охорони здоров’я, адже визначає швидкість, безпеку та якість руху інформаційних потоків для управління системою охорони здоров’я та реалізації медичних послуг.

Державно-управлінські фактори визначають сукупність детермінант впливу на прийняття та реалізацію державно-управлінських рішень щодо цифрової трансформації системи охорони здоров’я. Такі детермінанти обумовлені специфікою функціонування суб’єктів державного управління, їх взаємодією в процесах цифровізації системи охорони здоров’я. Причиною цього є полісуб’єктність державного управління системою охорони здоров’я. В контексті зазначеного пропонуємо визначати наступні види факторів впливу:

- інституційні - 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. Вплив інституційних факторів залежить від розподілу функцій та усунення дублювання повноважень між суб’єктами державного управління, закладами охорони здоров’я та ключовими зацікавленими сторонами, адже дані фактори визначають керованість і результативність процесу. Якщо інституційна спроможність суб'єктів є низькою, а механізми взаємодії між міністерствами неузгоджені, ефективність процесів цифрової трансформації буде низькою та хаотичною. В свою чергу, створення чіткої інституційної вертикалі дозволяє забезпечити планомірне масштабування реформи на всю країну.

- організаційні - 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. «В контексті цифровізації охорони здоров’я стандартизація виявляється необхідною в багатьох видах діяльності. Це включає реєстри установ для систематизації та управління інформацією про медичні заклади; реєстри

постачальників медичних послуг для визначення та контролю якості послуг, які надаються; реєстри кадрових ресурсів охорони здоров’я для ведення даних про медичних працівників та їх кваліфікацію; реєстри національних схем страхування для контролю за страховим покриттям та обліку пацієнтів; схеми унікальної ідентифікації громадян для точної ідентифікації пацієнтів та ведення їх медичних записів; каталоги основних лікарських засобів та товарів для контролю за наявністю та доступністю медичних продуктів; кодування захворювань для класифікації та аналізу захворювань з метою стандартизації лікування; значення лабораторних параметрів для однозначного розуміння результатів медичних досліджень; термінологічні списки для визначення загальноприйнятих термінів та термінології в охороні здоров’я; функціональна сумісність пристроїв для забезпечення сумісності та ефективної взаємодії між різними медичними пристроями та системами» [161]. Організаційні фактори визначають гнучкість та адаптивність системи, в той же час цифрова трансформація вимагає модернізації організаційних положень щодо приведення у відповідність до єдиних, логічних стандартів усіх управлінських, медичних, логістичних, фінансових та інших процесів.

- інформаційні - 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. Інформаційні чинники є базою для якості та обґрунтованості державного управління. Ефективний інформаційний супровід обмежує прийняття рішення на основі застарілих або сфальсифікованих паперових звітів. Завдяки прозорому та швидкому обміну інформацією держава бачить реальну картину про функціонування системи охорони здоров’я. Це перетворює інформаційну взаємодію на стратегічний ресурс розвитку всієї галузі.

Безпекові фактори визначають стійкість, захищеність та життєздатність усієї системи охорони здоров’я в умовах постійних внутрішніх і зовнішніх загроз, та особливо її функціонування у віртуальному просторі. Безпека виступає не просто як технічна вимога, а як фундаментальна умова збереження національної безпеки держави в цілому та безпеки лікаря, медичного персоналу та пацієнтів як з фізичної точки зору так і з ментальної. Безпековими факторами, зважаючи на властивості системи охорони здоров’я та цифрової трансформації є наступні:

- інформаційно-безпекові фактори - 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. Інформаційно-безпекові фактори впливають на рівень довіри до цифрової системи охорони здоров’я. «Національні системи охорони здоров’я складаються з різноманітних складних компонентів з широким спектром даних, які збираються, обробляються та використовуються для забезпечення ефективного функціонування системи охорони здоров’я. Ці дані охоплюють не лише медичну інформацію про пацієнтів, а й дані з епідеміологічних досліджень, реєстрації подій цивільного стану, статистики народжуваності та смертності, а також різні інші аспекти, що впливають на здоров’я та добробут нації» [9]. Держава має гарантувати, що медична інформація про пацієнтів, персональна інформація про медичний персонал та інших осіб не стануть доступними третім особам, дані не будуть підроблені чи стерті, адже це може дискредитувати цифрову трансформацію системи охорони здоров’я, і як наслідок спричинити суспільний та політичний опір.

- кібербезпекові - 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. «Однією з ключових загроз є недостатній рівень кібербезпеки. Із переходом до цифрових реєстрів та інтеграції персональних даних з різних джерел (соціальних, податкових, демографічних, медичних) зростає ризик витоків, зловживань і несанкціонованого доступу» [66]. Цифрова система охорони здоров’я є чутливою до кібератак, як і будь-яка інша цифрова система, проте в даній галузі кібератаки є вкрай небезпечними, адже можуть спричинити ризик для життя людини, через блокування роботи закладів охорони здоров’я або ж інформаційно-комутаційних систем взаємодії лікаря та пацієнта. Держава має розробити організаційні, правові заходи впровадження інструментів, спрямованих на мінімізацію кіберризиків.

- медико-безпекові - 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. Цифрова трансформація системи охорони здоров’я може як спричинити сукупність ризиків через використання інформаційних технологій так і забезпечити безперервний дистанційний моніторинг критичних пацієнтів і захистити самих медиків від юридичних ризиків, створюючи об'єктивний цифровий слід кожної медичної маніпуляції.

Таким чином, визначена сукупність факторів впливає 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. Цифрова трансформація системи охорони здоров'я є не лише технічним оновленням інфраструктури, а виступає стратегічним інструментом оптимізації обмежених ресурсів держави, зниження соціальної напруги та гарантування національної безпеки.

1.2. Джерельна база наукового дослідження державного управління цифровою трансформацією системи охорони здоров'я

Стрімка цифровізація сфери охорони здоров'я супроводжується зростанням кількості наукових праць. Різноманітність відповідних досліджень зумовлює необхідність систематизації наукового доробку для визначення перспективних напрямків досліджень.

Для дослідження розвитку наукового дискурсу було сформовано вибірку публікацій із наукометричної бази Scopus за пошуковим запитом «digital healthcare systems» за 2007–2026 рр. У межах опрацювання отриманих даних проаналізовано динаміку кількості публікацій, їх розподіл за країнами, науковими установами, галузями знань і джерелами опублікування. Окрему увагу приділено показникам цитованості, джерелам фінансування, міжнародним науковим зв'язкам, найуживанішим термінам і зміні тематичних пріоритетів упродовж досліджуваного періоду. Для опрацювання та візуалізації результатів використано програмне забезпечення VOSviewer і пакет Bibliometrix.

Одним із показників розвитку наукового інтересу до цифрових систем охорони здоров'я є динаміка кількості відповідних публікацій (рис. 1.1).

Згідно з рис. 1.1, у 2007–2016 рр. публікаційна активність була низькою - щорічна кількість праць не перевищувала двох. Із 2017 р. розпочалося поступове зростання, яке суттєво прискорилося після 2020 р.: кількість публікацій збільшилася із 17 у 2021 р. до 50 у 2024 р. Максимальне значення зафіксовано у 2025 р. - 83 публікації, що майже у п'ять разів більше, ніж у 2021 р. Така динаміка свідчить про стрімке посилення уваги науковців до цифровізації охорони здоров'я. Зниження показника до 42 публікацій у 2026 р. не варто розглядати як сталий спад, оскільки дані взяті лише за перше півріччя та відображають публікації, проіндексовані на момент формування вибірки.

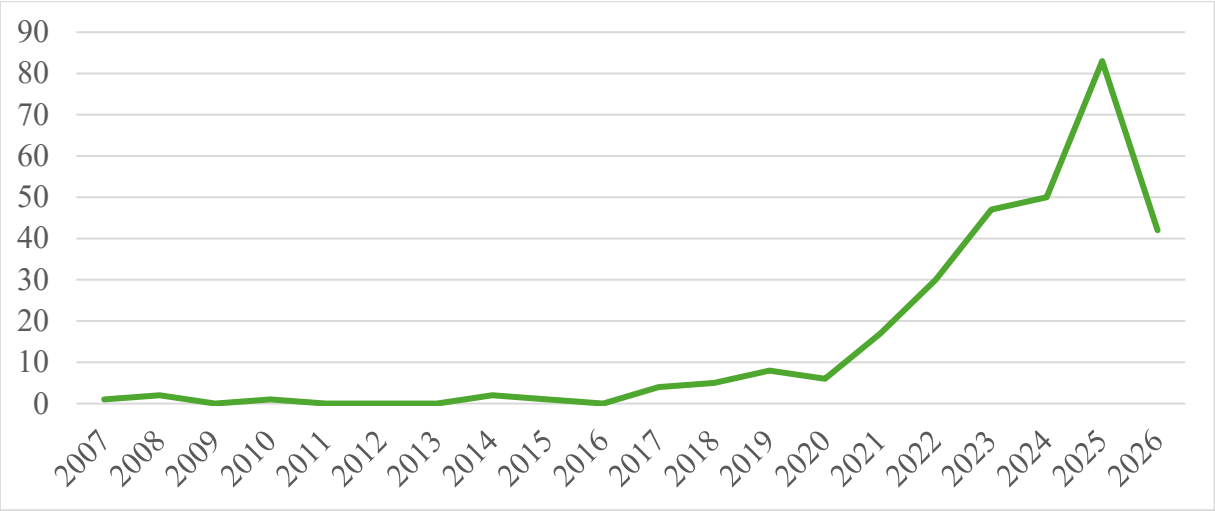


Рис. 1.1. Динаміка публікаційної активності за пошуковим запитом «digital healthcare systems» у наукометричній базі Scopus, 2007–2026 рр.

Джерело: побудовано автором

Зростання кількості публікацій зумовлює необхідність визначення основних напрямів, у межах яких розвиваються дослідження цифрових систем охорони здоров'я. Для цього побудовано мережу спільного виникнення термінів, яка відображає їх тематичну близькість, частоту використання та взаємозв'язки (рис. 1.2).

Мережа взаємозв'язків термінів підтверджує комплексний характер досліджень цифрових систем охорони здоров'я, які поєднують медичні, інформаційно-технологічні та безпекові аспекти. Центральне місце посідають питання застосування штучного інтелекту, медичних обчислень, цифрового надання медичної допомоги та захисту даних пацієнтів.

Виявлене поєднання технологічних і безпекових напрямів узгоджується з позицією ВООЗ, відповідно до якої під час розроблення та використання штучного інтелекту «етика і права людини мають перебувати в центрі його проєктування, впровадження та застосування» [149].

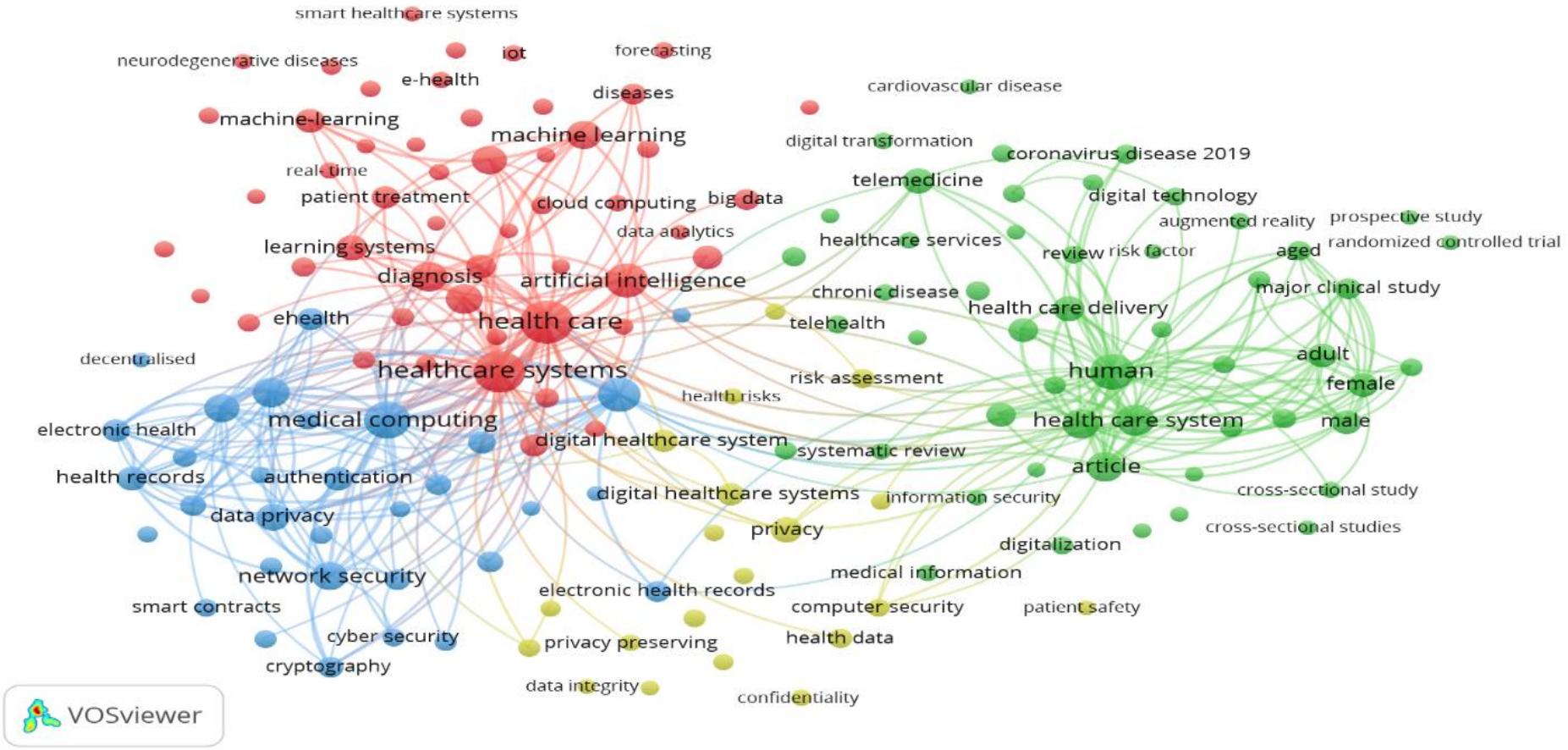


Рис. 1.2. Мережа спільного виникнення ключових слів у публікаціях за пошуковим запитом «digital healthcare systems» у наукометричній базі Scopus, 2007–2026 рр.

Джерело: сформовано автором за даними наукометричної бази Scopus із використанням програмного забезпечення VOSviewer

Для більш детального розкриття тематичної структури виявлені на рисунку взаємопов'язані терміни було систематизовано за чотирма основними кластерами, характеристику яких наведено в табл. 1.2.

Таблиця 1.2

Тематичні кластери досліджень цифрових систем охорони здоров'я

Кластер	Основні терміни	Тематична спрямованість
Червоний	healthcare systems, health care, artificial intelligence, machine learning, diagnosis, big data, cloud computing, data analytics, e-health, IoT, patient treatment	Застосування штучного інтелекту, машинного навчання, великих даних і хмарних технологій у діагностиці, лікуванні та функціонуванні систем охорони здоров'я
Синій	medical computing, ehealth, electronic health, health records, data privacy, authentication, network security, cyber security, cryptography, smart contracts	Інформаційно-технологічна інфраструктура електронної охорони здоров'я, кібербезпека, автентифікація та захист медичних даних
Зелений	human, health care system, health care delivery, telemedicine, healthcare services, digital technology, digital transformation, chronic disease, coronavirus disease 2019, adult, female, male	Практичне використання цифрових технологій у наданні медичної допомоги, телемедицині, клінічних дослідженнях і роботі з різними групами пацієнтів
Жовтий	privacy, information security, confidentiality, data integrity, privacy preserving, health data, electronic health records, risk assessment, patient safety, computer security	Забезпечення конфіденційності, цілісності та безпеки медичної інформації, оцінювання ризиків і захист приватності пацієнтів

Дані табл. 1.2 свідчать, що розвиток цифрових систем охорони здоров'я відбувається за чотирма взаємопов'язаними напрямами: впровадження інтелектуальних технологій у медицину; розвиток цифрової інфраструктури; практичне використання телемедицини та електронних медичних сервісів; забезпечення конфіденційності й кібербезпеки. Отже, подальша цифровізація охорони здоров'я потребує одночасного розвитку технологічних рішень, медичних практик і механізмів захисту інформації.

Актуальність захисту медичної інформації підтверджується і сучасними нормативними тенденціями. Регламентом ЄС 2025/327 Європейський простір даних охорони здоров'я створюється на основі «спільних правил, стандартів,

інфраструктури та системи управління» [248]. Його завданням є забезпечення контрольованого, безпечного та сумісного використання електронних медичних даних.

Визначені тематичні кластери характеризують загальну структуру досліджень, однак не відображають зміну наукових пріоритетів у часі. Тому доцільно простежити еволюцію найбільш поширених тематичних напрямів упродовж досліджуваного періоду, що представлено на рис. 1.3.

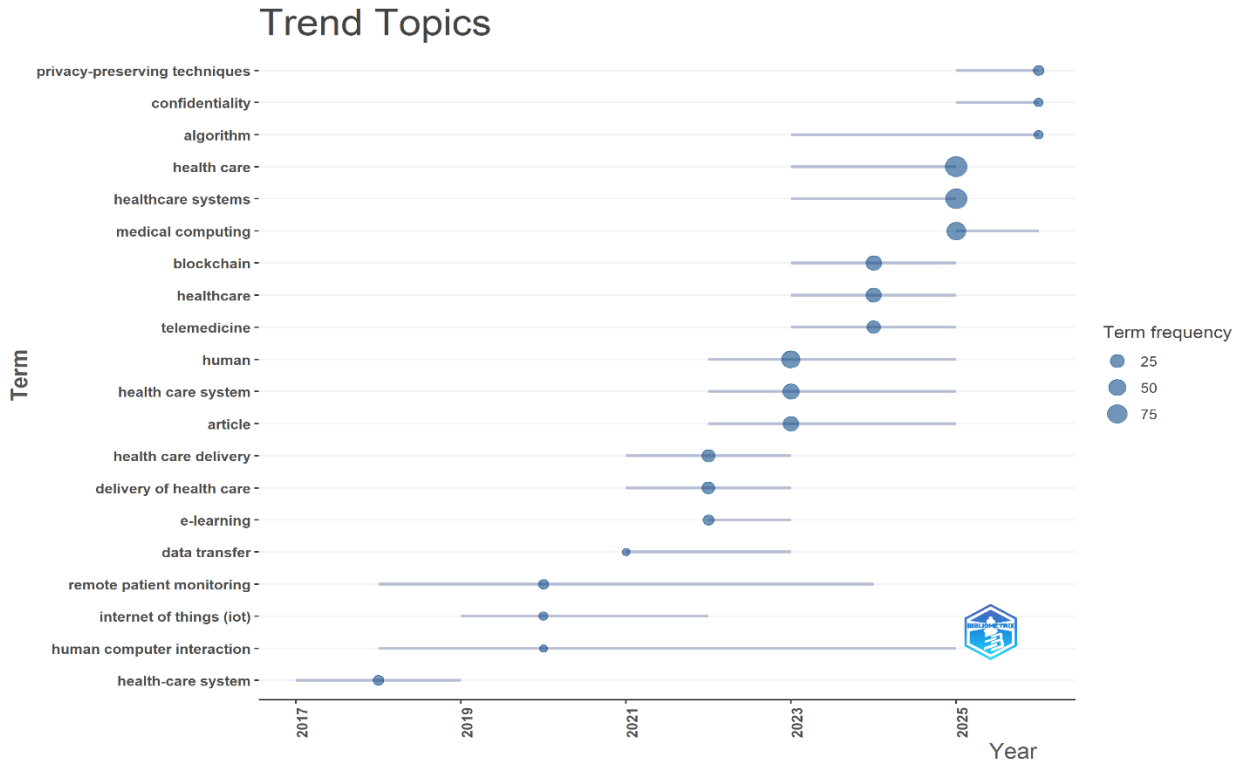


Рис. 1.3. Динаміка тематичних трендів у публікаціях за пошуковим запитом «digital healthcare systems» у наукометричній базі Scopus, 2017–2026 рр.

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

Дані рис. 1.3 свідчать про поступову зміну тематичних пріоритетів. На початковому етапі дослідники зосереджувалися на загальних питаннях функціонування електронних систем охорони здоров'я та взаємодії людини з комп'ютером. У 2019-2022 рр. актуальності набули Інтернет речей, дистанційний моніторинг пацієнтів, передавання даних, електронне навчання

та цифрове надання медичної допомоги. У 2023–2025 рр. увага змістилася до телемедицини, блокчейну, медичних обчислень і комплексного розвитку систем охорони здоров'я. Найновіші напрями пов'язані з алгоритмами, конфіденційністю та технологіями збереження приватності. Отже, дослідження поступово переходять від упровадження окремих цифрових рішень до забезпечення їх надійності, безпеки та захисту медичних даних.

Зростання уваги до електронних медичних записів і сумісності цифрових систем підтверджується результатами S. Palojoki, L. Lehtonen, R. Vuokko, які зазначають, що «семантична сумісність полегшує обмін медичними даними та доступ до них» [231]. Вона дає змогу використовувати інформацію в різних електронних системах без втрати її змісту.

Визначення часової еволюції тематичних напрямів доцільно доповнити оцінюванням частоти використання окремих термінів. Це дає змогу встановити поняття, які формують змістове ядро досліджень цифрових систем охорони здоров'я.

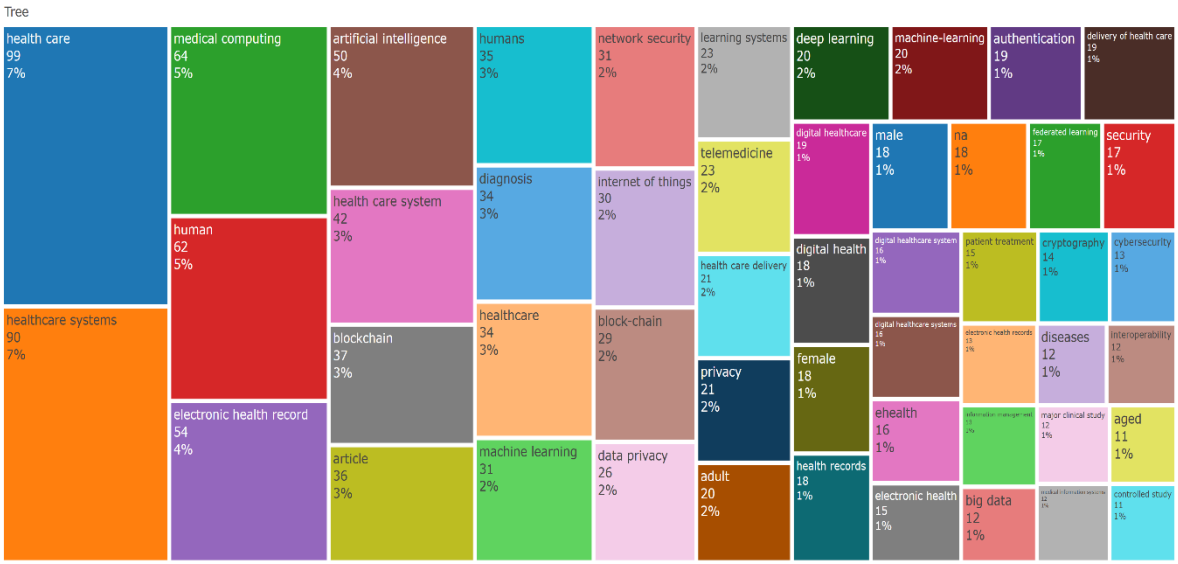


Рис. 1.4. Найбільш уживані терміни в публікаціях за пошуковим запитом «digital healthcare systems» у наукометричній базі Scopus, 2007–2026 рр.

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

Як свідчать дані рис. 1.4, найчастіше в публікаціях використовуються терміни «health care» - 99 згадувань (7%), «healthcare systems» - 90 (7%), «medical computing» - 64 (5%), «human» - 62 (5%) та «electronic health record» - 54 (4%). Вагоме місце також посідають терміни «artificial intelligence» - 50 згадувань (4%), «health care system», «blockchain», «article», «diagnosis» і «healthcare» - по 3 %.

Помітною є частота використання понять «machine learning», «network», «security», «internet of things», «data privacy», «telemedicine», «privacy», «deep learning», «authentication» і «federated learning». Виходячи з цього, можемо стверджувати, що змістове ядро досліджень поєднує три основні складові: цифрову організацію медичної допомоги, використання інтелектуальних технологій та захист медичної інформації.

Водночас у вибірці наявні різні варіанти написання близьких або однакових понять, зокрема «blockchain» і «block-chain», «machine learning» і «machine-learning», «human» і «humans», «health care» і «healthcare». Загалом рисунок підтверджує міждисциплінарність досліджуваної проблематики та провідну роль штучного інтелекту, медичних обчислень, електронних медичних записів і технологій інформаційної безпеки.

Поряд із визначенням тематичної структури публікацій важливим є дослідження географії їх походження. Це дає змогу встановити країни, науковці яких найактивніше працюють над проблематикою цифрових систем охорони здоров’я, та визначити основні центри формування відповідного наукового доробку (рис. 1.5).

Як свідчать дані рис. 1.5, беззаперечним лідером за кількістю публікацій є Індія - 113 документів, що у 3,3 раза перевищує показник Сполучених Штатів Америки, які посідають друге місце із 34 публікаціями. Наступні позиції займають Південна Корея – 25 публікацій, Велика Британія – 22 публікації, Австралія – 21 публікація і Китай - 20

публікацій. Серед інших активних країн представлені Саудівська Аравія – 18 публікацій, Німеччина – 16 публікацій, Малайзія – 15 публікацій, Італія та Норвегія - по 11 публікацій, Фінляндія і Пакистан - по 10 документів.

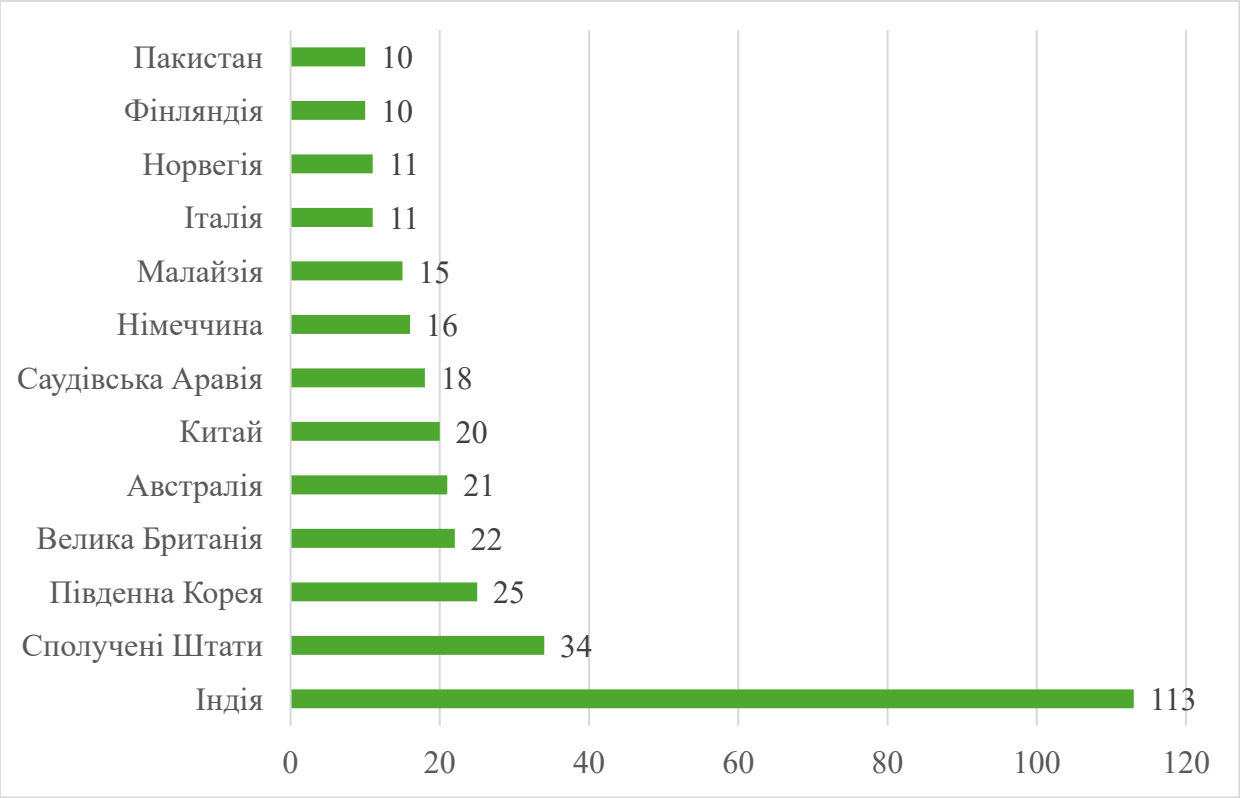


Рис. 1.5. Розподіл публікацій за країнами за пошуковим запитом «digital healthcare systems» у наукометричній базі Scopus, 2007–2026 рр.

Джерело: побудовано автором

Отримані результати засвідчують домінування країн Азії, передусім Індії, Південної Кореї та Китаю, у дослідженні цифрових систем охорони здоров'я. Водночас до переліку провідних країн входять представники Північної Америки, Європи та Австралії, що підтверджує глобальний характер цієї проблематики.

Кількість публікацій характеризує наукову активність країн, однак не повною мірою відображає вплив оприлюднених результатів. Для оцінювання їх затребуваності в академічному середовищі доцільно проаналізувати розподіл цитувань за країнами, представлений на рис. 1.6.

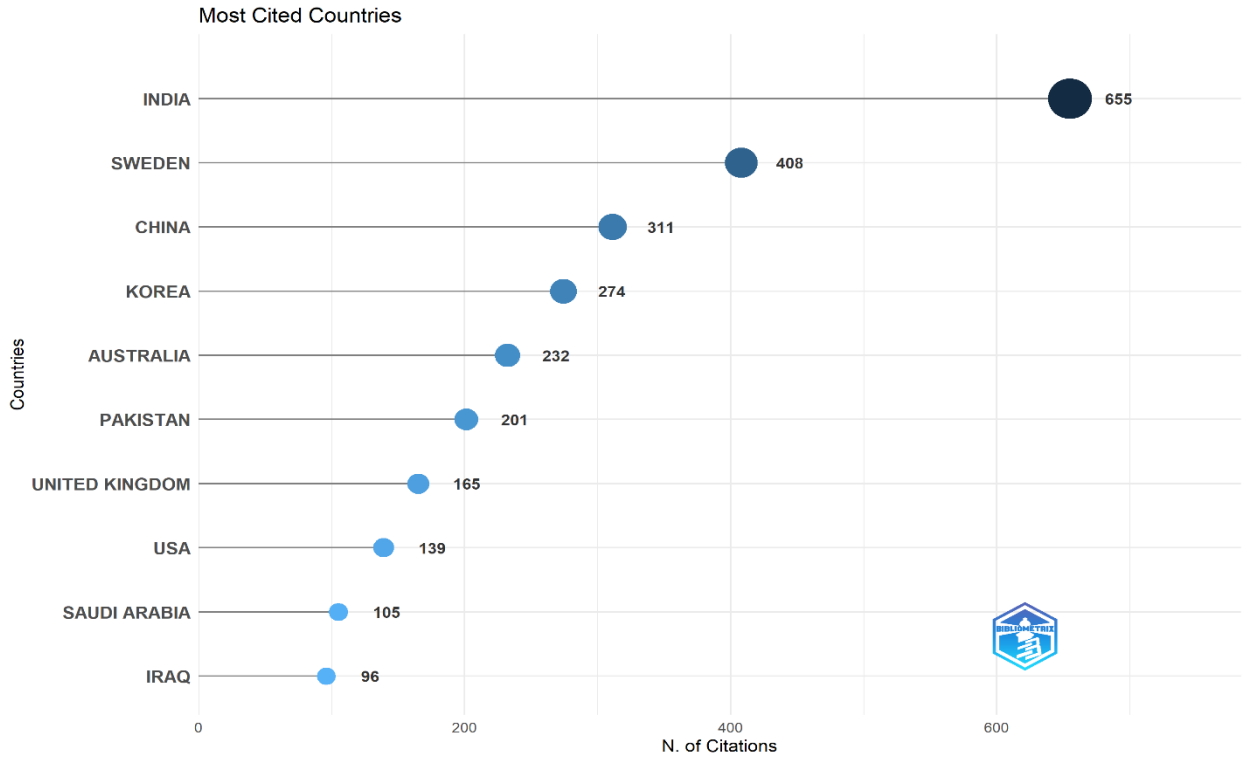


Рис. 1.6. Розподіл цитувань публікацій за країнами за пошуковим запитом «digital healthcare systems» у наукометричній базі Scopus, 2007–2026 рр.

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

Як свідчать дані рис. 1.6, найбільшу кількість цитувань отримали публікації дослідників з Індії - 655. Друге місце посідає Швеція із 408 цитуваннями, третє - Китай із 311. Високі показники також мають Південна Корея - 274, Австралія - 232 та Пакистан - 201 цитування. Показники Великої Британії становлять 165 цитувань, США - 139, Саудівської Аравії - 105, Іраку - 96.

Порівняння результатів із кількістю публікацій свідчить, що публікаційна активність не завжди прямо визначає рівень наукового впливу. Зокрема, Швеція не входить до трійки лідерів за кількістю документів, але посідає друге місце за цитованістю. Пакистан, маючи 10 публікацій, випереджає за кількістю цитувань Велику Британію та США, які опублікували значно більше праць. Натомість США посідають друге місце за кількістю

документів, але лише восьме - за цитованістю. Отже, найбільш помітний науковий вплив у досліджуваній сфері мають Індія, Швеція, Китай, Південна Корея та Австралія.

Необхідність міжнародної взаємодії у цій сфері підкреслює Генеральний директор ВООЗ Тедрос Адханом Гебреєсус: «Майбутнє охорони здоров'я - цифрове. Але для втілення цього бачення потрібні і ресурси, і співпраця» [110].

Високі показники публікаційної активності та цитованості окремих країн значною мірою формуються під впливом міжнародного наукового співробітництва. Для визначення його структури побудовано мережу співавторських зв'язків між країнами (рис. 1.7).

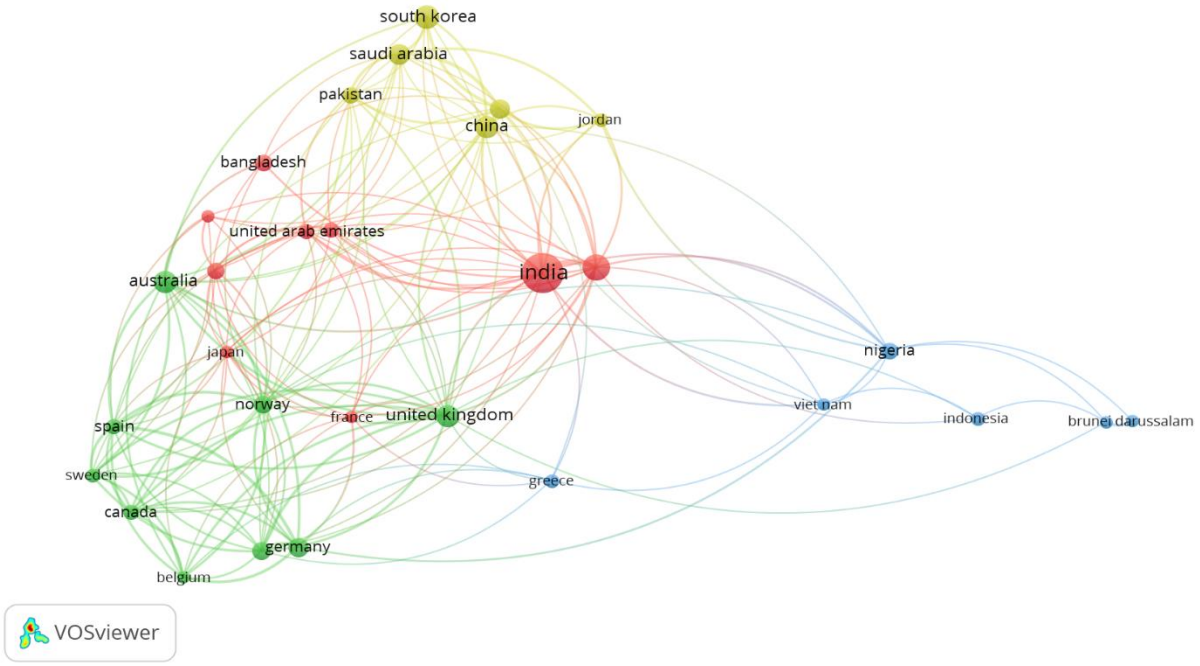


Рис. 1.7. Мережа міжнародного наукового співробітництва за публікаціями, відібраними за пошуковим запитом «digital healthcare systems» у наукометричній базі Scopus, 2007–2026 рр.

Джерело: сформовано автором за даними наукометричної бази Scopus із використанням програмного забезпечення VOSviewer

Мережа міжнародного співавторства характеризується наявністю декількох взаємопов'язаних груп країн. Найбільшим і найвпливовішим вузлом є Індія, яка виконує роль сполучної ланки між азійськими, європейськими, близькосхідними й африканськими дослідниками. Водночас щільні зв'язки простежуються між країнами Європи, а також між державами Азії та Близького Сходу.

Для детальнішого представлення структури міжнародної взаємодії країни систематизовано відповідно до кольорового групування, сформованого програмою VOSviewer. Склад і загальну характеристику виявлених кластерів наведено в таблиці 1.3.

Таблиця 2.3

Кластери міжнародного наукового співробітництва у дослідженні цифрових систем охорони здоров'я

Кластер	Країни, що входять до кластера	Центральна країна	Характеристика співробітництва
Червоний	Індія, Об'єднані Арабські Емірати, Бангладеш, Японія, Франція	Індія	Найбільш розгалужений міжрегіональний кластер, який забезпечує взаємодію між науковцями Південної Азії, Близького Сходу та Європи
Зелений	Велика Британія, Німеччина, Норвегія, Швеція, Іспанія, Бельгія, Канада, Австралія	Велика Британія та Німеччина	Щільна мережа співпраці між європейськими країнами з активним залученням Австралії та Канади
Жовтий	Китай, Південна Корея, Саудівська Аравія, Пакистан, Йорданія	Китай	Азійсько-близькосхідний кластер, у якому розвинені зв'язки між країнами Східної та Південної Азії і державами Близького Сходу
Синій	Нігерія, В'єтнам, Індонезія, Бруней-Даруссалам, Греція	Нігерія	Порівняно віддалений кластер, який об'єднує країни Африки, Південно-Східної Азії та Європи й має зв'язки з основними центрами мережі

Джерело: систематизовано автором за результатами візуалізації даних Scopus із використанням програмного забезпечення VOSviewer

Дані таблиці 1.3 підтверджують, що міжнародне співробітництво у сфері цифрових систем охорони здоров'я формується переважно навколо Індії, Великої Британії, Німеччини та Китаю. Найбільш щільними є зв'язки всередині європейського та азійсько-близькосхідного кластерів, тоді як Індія забезпечує взаємодію між різними регіональними групами. Синій кластер займає більш периферійне положення, проте розширює географію досліджень завдяки залученню країн Африки та Південно-Східної Азії.

Розвиток міжнародного наукового співробітництва та реалізація досліджень цифрових систем охорони здоров'я значною мірою залежать від належної фінансової підтримки. Тому важливим є визначення організацій, фондів і установ, які найактивніше фінансують публікації за досліджуваною проблематикою (рис. 1.8).

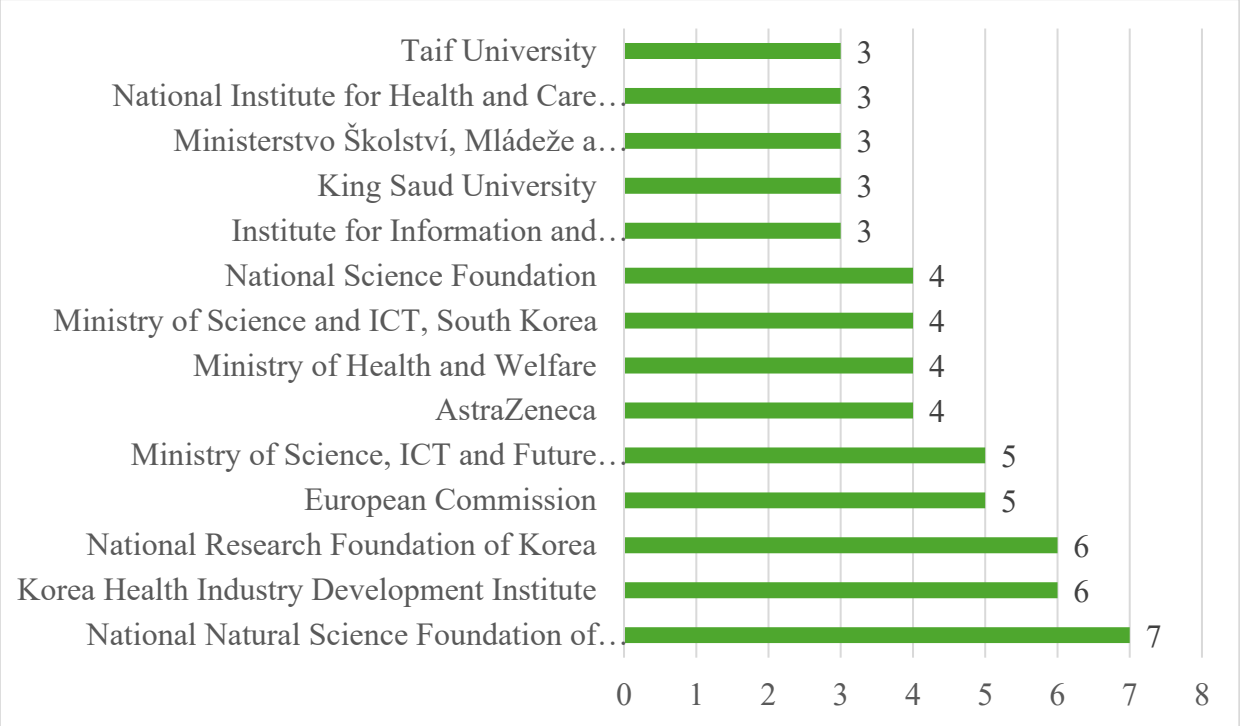


Рис. 1.8. Джерела фінансування публікацій за пошуковим запитом «digital healthcare systems» у наукометричній базі Scopus, 2007–2026 рр.

Джерело: побудовано автором

Згідно з рис. 1.8, провідним джерелом фінансування є National Natural Science Foundation of China, за підтримки якого опубліковано 7 документів. По 6 публікацій профінансували Korea Health Industry Development Institute та National Research Foundation of Korea. Підтримку п’яти публікацій забезпечили European Commission і Ministry of Science, ICT and Future Planning. По чотири документи профінансували AstraZeneca, Ministry of Health and Welfare, Ministry of Science and ICT, South Korea та National Science Foundation. Інші представлені організації підтримали по три публікації.

Отже, серед провідних джерел фінансування переважають державні наукові фонди, міністерства та профільні установи Китаю і Південної Кореї. Це підтверджує важливу роль державної науково-технологічної політики у розвитку цифрових систем охорони здоров’я. Водночас присутність Європейської комісії, університетів, національних дослідницьких установ і компанії AstraZeneca свідчить про поєднання державного, наднаціонального, академічного та приватного фінансування відповідних досліджень.

Значення комплексного ресурсного забезпечення також відображено в Глобальній стратегії ВООЗ, відповідно до якої цифрові ініціативи мають спиратися на стратегію, що «інтегрує фінансові, організаційні, людські та технологічні ресурси» [165].

Поряд із визначенням провідних джерел фінансування доцільно встановити наукові установи, які роблять найбільший внесок у дослідження цифрових систем охорони здоров’я. Розподіл публікацій за організаційною належністю авторів дає змогу визначити основні інституційні центри розвитку цієї проблематики (рис. 1.9).

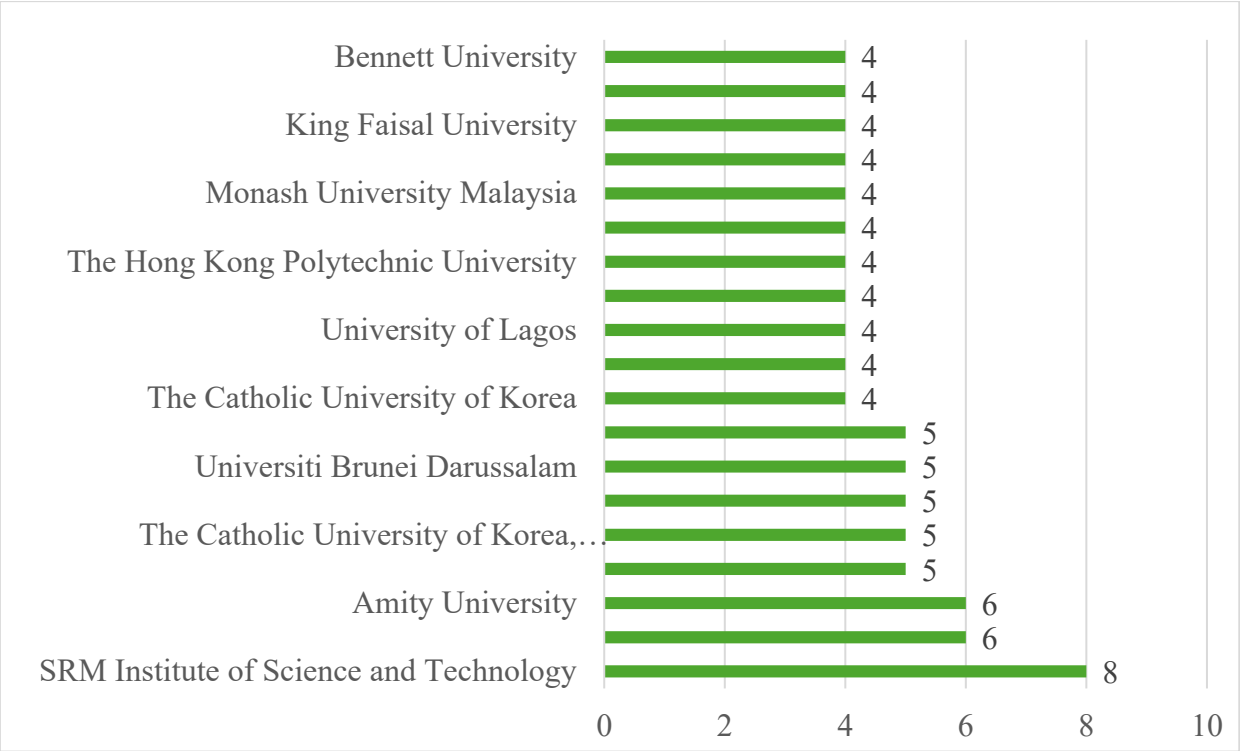


Рис. 1.9. Провідні наукові установи за кількістю публікацій за пошуковим запитом «digital healthcare systems» у наукометричній базі Scopus, 2007–2026 рр.

Джерело: побудовано автором

Згідно з рис. 1.9, найбільш продуктивною установою є SRM Institute of Science and Technology - 8 публікацій. Другу позицію поділяють The University of Jordan та Amity University, дослідники яких підготували по 6 документів. По 5 публікацій мають Seoul National University College of Medicine, The Catholic University of Korea, College of Medicine, SKKU School of Medicine, Universiti Brunei Darussalam та Raiganj University.

Ще низка установ представлена чотирма публікаціями, зокрема The Catholic University of Korea, Uppsala Universitet, University of Lagos, Universidade do Porto, The Hong Kong Polytechnic University, Oulun Yliopisto, Monash University Malaysia, University of Oxford, King Faisal University, Seoul National University Bundang Hospital і Bennett University.

Отримані результати засвідчують географічну різноманітність інституційного середовища, оскільки до переліку входять університети й медичні установи Індії, Йорданії, Південної Кореї, Брунею, Нігерії, Португалії, Фінляндії, Малайзії, Великої Британії та інших країн. Водночас особливо помітною є представленість індійських і південнокорейських установ. Це підтверджує провідну роль азійських наукових центрів та активну участь спеціалізованих медичних університетів у розвитку цифрових систем охорони здоров'я. Відносно невелика різниця між показниками більшості установ свідчить про відсутність надмірної концентрації публікацій в одному науковому центрі.

Визначення провідних наукових установ доцільно доповнити дослідженням джерел, у яких найчастіше публікуються результати робіт із цифрових систем охорони здоров'я (рис. 1.10).

Найбільшу кількість документів представлено у виданні Federated Learning for Digital Healthcare Systems - 11. Другу позицію займає серія Communications in Computer and Information Science - 6 публікацій. По 5 документів опубліковано у Lecture Notes in Networks and Systems, Scientific Reports, Sensors, Studies in Computational Intelligence та Studies in Health Technology and Informatics. У виданні Digital Health і серії Lecture Notes of the Institute for Computer Sciences представлено по 4 публікації, а в CEUR Workshop Proceedings - 3.

Структура провідних джерел підтверджує міждисциплінарний характер досліджень, оскільки охоплює медичні та технологічні журнали, книжкові серії, збірники й матеріали наукових конференцій. Значна представленість видань з комп'ютерних наук свідчить про переважання технологічного підходу до дослідження цифрових систем охорони здоров'я. Водночас присутність Scientific Reports, Sensors і Digital Health указує на поступове розширення публікацій у спеціалізованих медичних і міждисциплінарних журналах.

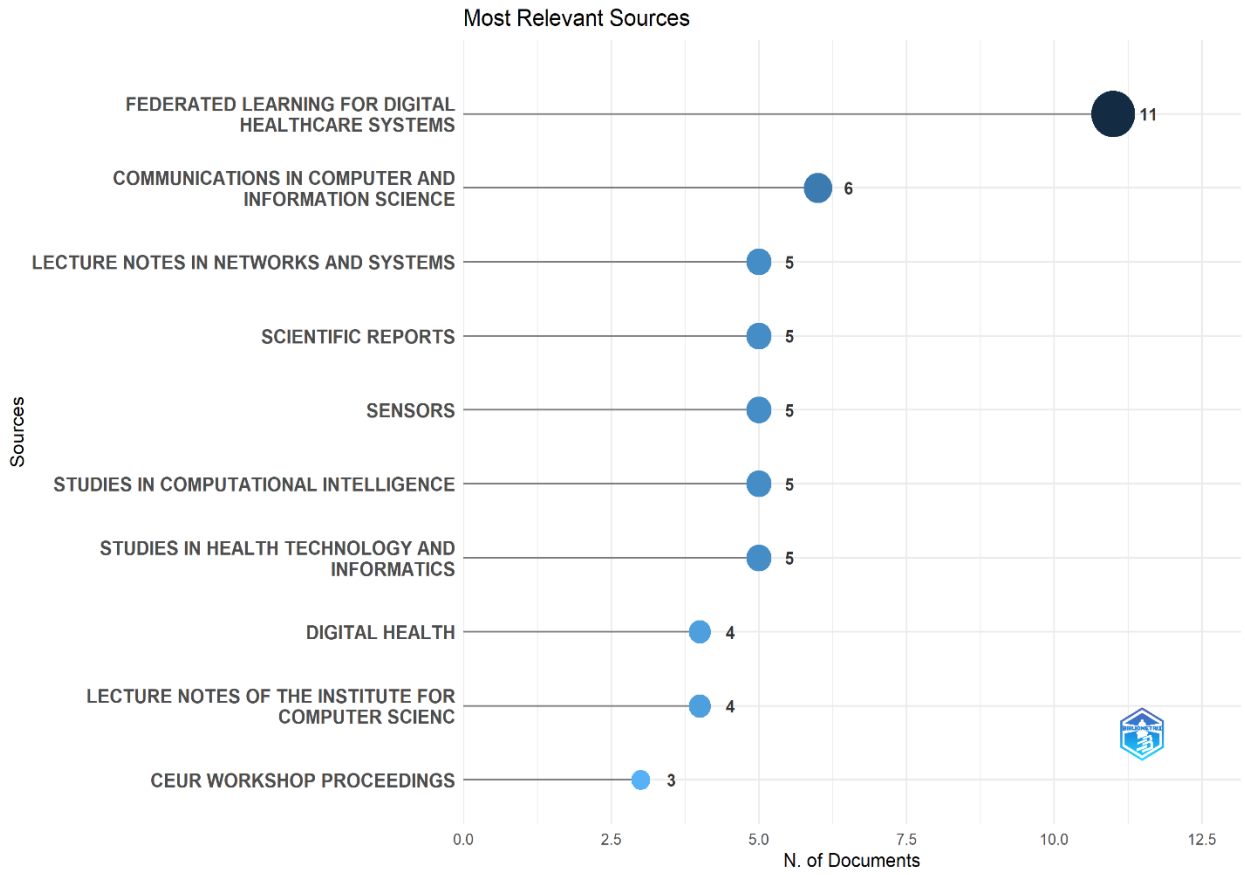


Рис. 1.10. Провідні джерела опублікування результатів досліджень за пошуковим запитом «digital healthcare systems» у наукометричній базі Scopus, 2007–2026 рр.

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

Визначення провідних джерел публікування доцільно доповнити дослідженням їхньої активності в часі. Це дає змогу встановити періоди появи відповідних видань у сформованій вибірці та простежити накопичення кількості опублікованих у них документів (рис. 1.11).

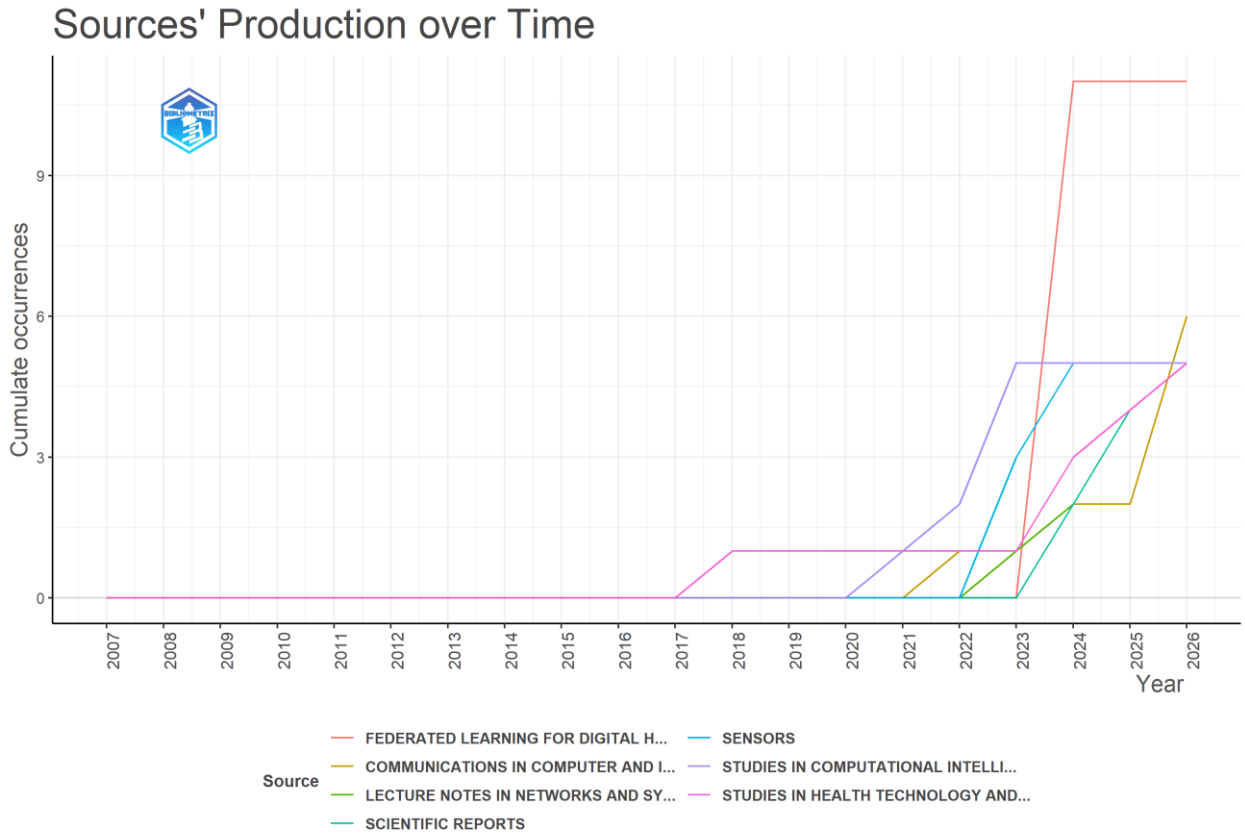


Рис. 1.11. Динаміка публікаційної активності провідних наукових джерел за пошуковим запитом «digital healthcare systems» у наукометричній базі Scopus, 2007–2026 рр.

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

Дані рис. 1.11 свідчать, що активне опублікування праць із цифрових систем охорони здоров'я у провідних джерелах розпочалося переважно після 2020 р. Найраніше у вибірці з'явилося видання Studies in Health Technology and Informatics: першу публікацію зафіксовано у 2018 р., а надалі їх кумулятивна кількість поступово зросла до п'яти.

Серія Studies in Computational Intelligence демонструвала активне зростання у 2021–2023 рр., після чого її показник стабілізувався на рівні п'яти публікацій. У Sensors основне збільшення відбулося у 2022–2024 рр. - до п'яти документів. Публікаційна активність Scientific Reports і Lecture Notes in

Networks and Systems посилилася після 2023 р., а Communications in Computer and Information Science характеризується помітним зростанням наприкінці досліджуваного періоду - до шести публікацій у 2026 р. Найстрімкішу динаміку демонструє Federated Learning for Digital Healthcare Systems, кумулятивний показник якого у 2024 р. досяг 11 документів і надалі залишався незмінним. Загалом рисунок підтверджує, що основна частина публікацій у провідних джерелах з'явилася протягом останніх кількох років, що свідчить про новизну та стрімкий розвиток досліджуваного питання.

Динаміка публікаційної активності провідних джерел підтверджує посилення наукового інтересу до цифрових систем охорони здоров'я. Водночас для повнішого розуміння структури досліджень необхідно визначити галузі знань, у межах яких представлено відповідні публікації (рис. 1.12).

Відповідно до рис. 1.12, найбільша частка публікацій припадає на комп'ютерні науки - 187 документів, або 29%. Другу позицію займає інженерія - 105 документів (16%), третю - медицина - 92 документи (14%). Сукупно ці три галузі формують близько 59% усіх галузевих віднесень, що підтверджує переважно технологічну та медичну спрямованість досліджень.

На науки про прийняття рішень припадає 35 документів (5%), на математику - 31 (5%). Бізнес, менеджмент і бухгалтерський облік представлені 21 публікацією, соціальні науки – 20 публікаціями, біохімія, генетика та молекулярна біологія і професії охорони здоров'я - по 19 документів. Частка кожного із цих напрямів становить приблизно 3 %. Решта публікацій належать до фізики, енергетики, економіки, медсестринства, матеріалознавства, хімії, фармакології, наук про навколишнє середовище та інших галузей.

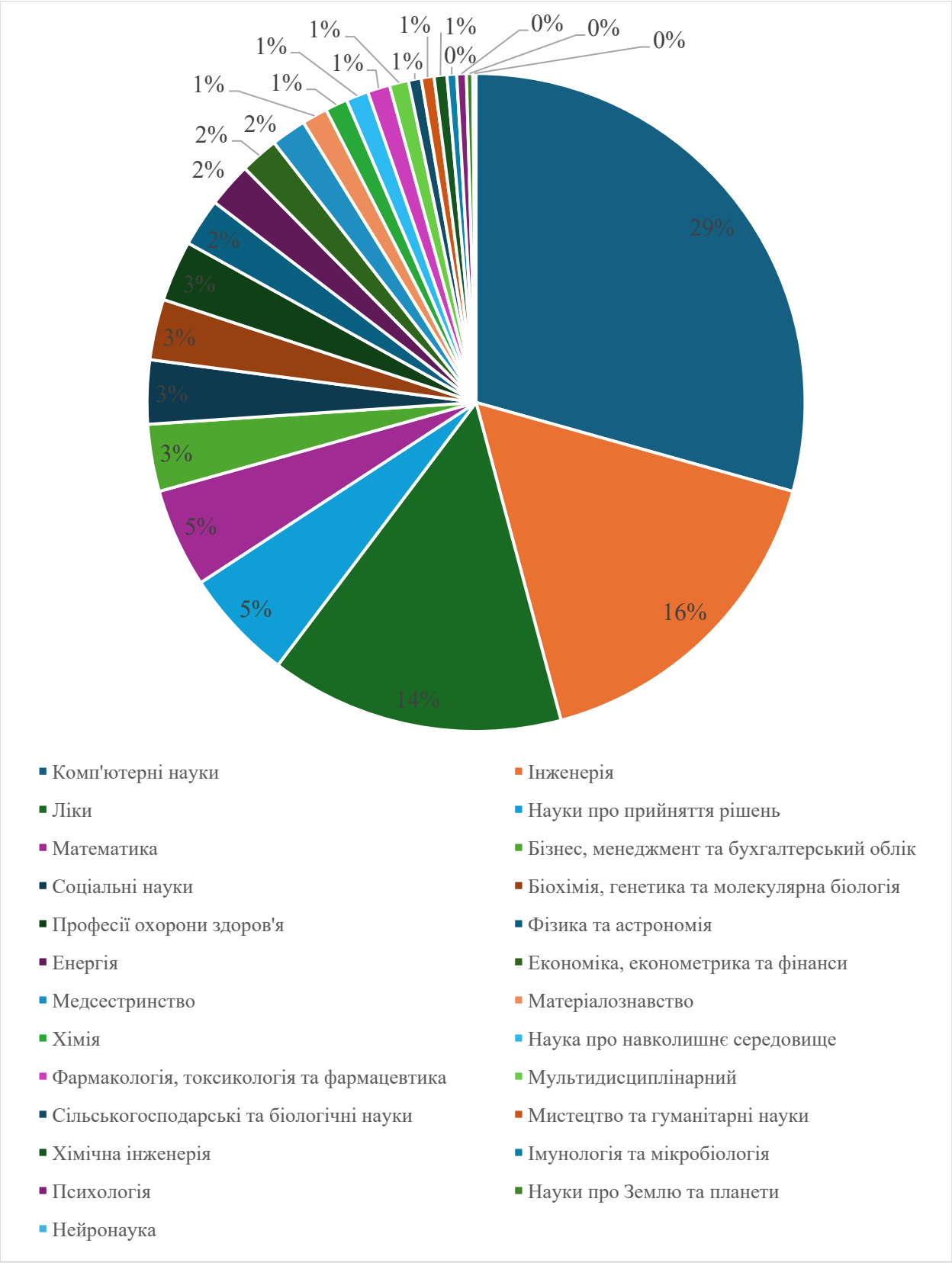


Рис. 1.12. Розподіл публікацій за галузями знань за пошуковим запитом «digital healthcare systems» у наукометричній базі Scopus, 2007–2026 рр.

Джерело: побудовано автором

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.

1.3. Понятійно-категоріальний апарат державного управління цифровою трансформацією системи охорони здоров'я

Будь-які трансформації в суспільному житті призводять до потреби наукового пошуку та обґрунтування теоретичного підґрунтя, яке передбачає розширення понятійно-категоріального апарату, або ж його зміни. Розвиток цифрових технологій, їх активне впровадження у сферу охорони здоров'я та трансформація механізмів державного управління актуалізують необхідність формування цілісного понятійно-категоріального апарату дослідження. Незважаючи на значну кількість наукових праць, присвячених цифровізації, цифровій трансформації та розвитку системи охорони здоров'я, у науковій літературі відсутній єдиний підхід до визначення базових понять, їх співвідношення та місця в системі державного управління. У зв'язку з цим виникає необхідність уточнення змісту ключових понять (система охорони здоров'я, цифрова трансформація, цифрова трансформація системи охорони здоров'я), встановлення взаємозв'язків між ними та визначення їх ролі у формуванні механізмів державного управління цифровою трансформацією системи охорони здоров'я. Формування логічно узгодженого понятійно-категоріального апарату створює методологічне підґрунтя для подальшого дослідження закономірностей, принципів, механізмів та інструментів державного управління цифровою трансформацією системи охорони здоров'я.

Питання змісту окремих понять та категорій державного управління системою охорони здоров'я були розглянуті в працях вчених: Терзі О.О., Шамич О.М., Швець Ю., Ліфінцев О.В., Проневич О.М., Джордж Вестерман, Дідьє Бонне, Ендрю МакАфі, Крістіан Матт, Томас Гесс, Александер Бенліан, Грегорі Віаль, Воржакова Ю.П., Сільченко В., Мандич О., Бабко Н., Лишенко М., Харчевнікова Л., Bouée C., Schaible S.,

Куйбіда В.С., Карпенко О.В., Наместнік В.В., Струтинська І.В., Нікітін Ю.О., Agarwal R., Gao G., DesRoches C., Jha A.K., Gopal G., Suter-Crazzolara C., Toldo L., Eberhardt W., Marques I.C., Ferreira J.J., Мартиненко О.В., Малярова Л.В., Бачук О.Р. та інші.

В контексті об’єктно-предметного поля дослідження, мети та завдань, є потреба в уточненні окремих понять, зокрема: система охорони здоров’я та цифрова трансформація системи охорони здоров’я.

Система охорони здоров’я. У Законі України «Основи законодавства України про охорону здоров’я» [35] міститься наступне тлумачення системи охорони здоров’я: «охорона здоров’я — це система заходів, що здійснюються органами державної влади та органами місцевого самоврядування, їх посадовими особами, закладами охорони здоров'я, фізичними особами-підприємцями, медичними та фармацевтичними працівниками, громадськими об'єднаннями і громадянами з метою збереження та відновлення фізіологічних і психологічних функцій, оптимальної працездатності та соціальної активності людини при максимальній біологічно можливій індивідуальній тривалості її життя» [35]. Нормативне визначення є базовим для правового регулювання сфери охорони здоров'я та комплексно визначає суб'єктів і кінцеву мету їх діяльності. Водночас охорона здоров’я розглядається виключно як система заходів, що акцентує увагу на функціональному аспекті, але не розкриває її як складну соціально-економічну систему та об’єкт державного управління.

Юридичний підхід міститься в науковій праці Терзі О.О. [71]. Так, автор зазначає, що «Охорона здоров’я – це система (сукупність) взаємопов'язаних і взаємозалежних заходів політичного, правового, організаційного, фінансового, соціально-економічного та медичного характеру, які здійснюються органами державної влади та недержавних організацій з метою

забезпечення довготривалого активного фізичного і психічного життя людини» [71]. Перевагою підходу є розширення змісту охорони здоров’я через включення політичних, правових, організаційних, фінансових та соціально-економічних заходів, що підкреслює її міжгалузевий характер. Разом із тим визначення зберігає традиційний функціональний підхід, ототожнюючи охорону здоров’я із сукупністю заходів, не розкриваючи внутрішню структуру системи та механізми її функціонування.

Шамич О.М. [75] пропонує розглядати охорону здоров’я як «систему заходів, спрямованих на збереження, зміцнення, розвиток та, у разі порушення, відновлення максимально досяжного рівня фізичного й психічного стану людського організму, які зобов'язані здійснювати органи державної влади, органи місцевого самоврядування, громадські організації, а також людина і населення в інтересах кожної особи та суспільства загалом» [75]. Автор акцентує увагу на широкому колі суб’єктів, відповідальних за охорону здоров’я, включаючи державу, місцеве самоврядування, громадські організації та саму людину, що відображає соціальну природу досліджуваного явища. Проте визначення також характеризує охорону здоров’я як систему заходів, залишаючи поза увагою її інституційну, управлінську та організаційну складові.

Швець Ю. [76] вказує, що «охорона здоров’я - це система правових, соціально-економічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження здоров'я людини; у широкому значенні — це сукупність заходів політичного, економічного, правового, соціального, культурного, наукового, медичного, санітарно-гігієнічного та протиепідемічного характеру, спрямованих на збереження і зміцнення здоров'я, підтримання довголітнього активного життя та надання медичної допомоги в разі його втрати» [76]. Запропонований підхід є одним із найбільш комплексних, оскільки охоплює політичні, економічні, правові, соціальні, культурні, наукові та медичні аспекти охорони здоров’я.

Водночас автор фактично розширює перелік заходів, не переходячи до розуміння охорони здоров’я як цілісної системи із взаємопов’язаними елементами, суб’єктами, ресурсами та механізмами функціонування.

Ліфінцев О.В. [25] наводить наступний зміст охорони здоров’я: «Охорона здоров’я - це система законодавчо регламентованих заходів з боку спеціально уповноважених суб’єктів, що провадять медичну практику та спрямовані на подання населенню послуг медичного характеру» [25]. Перевагою визначення є акцент на нормативно-правовому регулюванні медичної діяльності та ролі спеціально уповноважених суб’єктів. Разом із тим запропонований підхід є досить вузьким, оскільки фактично зводить охорону здоров’я до процесу надання медичних послуг, не враховуючи профілактичний, управлінський, соціальний, фінансовий та міжгалузевий компоненти.

Проневич О.М. [61] вказує, що поняття «охорона здоров’я» має полісемантичний характер, оскільки охоплює як медицину, так і низку інших сфер державної відповідальності, пов'язаних із забезпеченням фізичного і психічного здоров'я людей, їхнього соціального благополуччя та активного довголіття. Автор обґрунтовано підкреслює полісемантичний характер поняття «охорона здоров’я», вказуючи на його міжгалузеву природу та взаємозв’язок із різними напрямами державної діяльності. Разом із тим наведена характеристика має переважно концептуальний характер і не розкриває структурних елементів охорони здоров’я та особливостей її функціонування як системи.

Проведений аналіз свідчить, що більшість наукових підходів та нормативне визначення трактують охорону здоров’я переважно як систему заходів, спрямованих на збереження, зміцнення та відновлення здоров’я населення. Відмінності між наведеними підходами полягають насамперед у переліку суб’єктів, видах заходів та цілях їх реалізації, однак їх об'єднує

функціональне розуміння охорони здоров’я. Водночас такі підходи недостатньо розкривають її як складну динамічну систему, не характеризують внутрішню структуру, взаємозв’язки між елементами, ресурсне забезпечення, інституційні механізми та особливості державного управління. Крім того, наведені підходи сформувалися переважно в умовах традиційної моделі функціонування сфери охорони здоров'я та не враховують сучасні процеси цифрової трансформації, інтеграції цифрових технологій, інформаційних систем і штучного інтелекту у її функціонування. Це обумовлює необхідність переходу від функціонального розуміння охорони здоров'я як сукупності заходів до її розгляду як системи охорони здоров’я - багаторівневої соціально-економічної системи, 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 громадянського 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 системи охорони здоров’я. Поняття цифрової трансформації є досить дискусійним і сьогодні розглядається вченими з різних точок зору:

- Джордж Вестерман, Дідьє Бонне, Ендрю МакАфі [276] вказують, що цифрова трансформація - «це використання технологій для радикального поліпшення показників діяльності підприємства (organization performance), що охоплює три ключові напрями: взаємодію зі споживачами, оптимізацію операційних процесів та трансформацію

бізнес-моделей» [276]. Автори розглядають цифрову трансформацію як використання технологій для радикального поліпшення результатів діяльності організації через зміну взаємодії зі споживачами, операційних процесів і бізнес-моделей. Перевагою підходу є акцент не на самому впровадженні технологій, а на суттєвому покращенні діяльності організації. Водночас визначення має виразну підприємницьку спрямованість, тому недостатньо враховує суспільні цілі, публічні інтереси, інституційні зміни та особливості державного управління.

- Крістіан Матт, Томас Гесс, Александер Бенліан [210] визначають цифрову трансформацію як «центральну концепцію, що інтегрує координацію, пріоритизацію та реалізацію цифрових перетворень у межах підприємства, охоплюючи зміни бізнес-процесів, продуктів, організаційної структури та управлінських концепцій під впливом нових цифрових технологій» [210]. У цьому підході цифрова трансформація постає як інтегруюча концепція, що охоплює координацію, пріоритизацію та реалізацію цифрових змін у процесах, продуктах, організаційній структурі й управлінських підходах. Сильною стороною визначення є системне розуміння цифрової трансформації та включення до її змісту управлінської координації. Разом із тим об’єктом трансформації залишається підприємство, а мета, суб’єкти та суспільні наслідки цифрових змін чітко не визначені.

- Грегорі Віаль [269] вказує, що «цифрова трансформація - це процес, метою якого є вдосконалення сутності (підприємства, організації) шляхом ініціювання значущих змін її властивостей через поєднання інформаційних, обчислювальних, комунікаційних технологій та технологій зв’язку» [269]. Автор визначає цифрову трансформацію як процес значущої зміни властивостей певної сутності шляхом поєднання інформаційних, обчислювальних, комунікаційних технологій і технологій зв’язку. Перевагою

є універсальність дефініції, оскільки вона може застосовуватися не лише до підприємств, а й до організацій та складних систем. Особливо важливим є акцент на зміні властивостей об’єкта, що дає змогу відмежувати цифрову трансформацію від звичайного впровадження окремих технологій. Водночас визначення не розкриває цілеспрямованість, механізми управління, суб’єктів і результати такого процесу.

- Воржакова Ю.П. [8] пропонує під цифровою трансформацією розуміти «процес переходу на новий рівень ведення бізнесу зі зміною моделей функціонування, управління і бізнес-процесів з використанням сучасних цифрових технологій в усіх сферах діяльності» [8]. Цифрова трансформація трактується як перехід на новий рівень ведення бізнесу через зміну моделей функціонування, управління та бізнес-процесів із використанням цифрових технологій. Позитивним є розуміння трансформації як переходу до якісно нового стану, а не як локальної технологічної модернізації. Проте визначення обмежене бізнес-середовищем і не враховує інституційних, соціальних, правових та державно-управлінських змін.

- Сільченко В. [65] вказує, що «цифрова трансформація — це процес переходу до нових способів діяльності підприємства шляхом впровадження цифрових технологій у бізнес-процеси, що передбачає не лише встановлення сучасного обладнання, а й зміну моделей ведення бізнесу» [65]. Автор акцентує увагу на переході підприємства до нових способів діяльності та наголошує, що цифрова трансформація не зводиться до встановлення сучасного обладнання, а передбачає зміну бізнес-моделей. Такий підхід правильно відмежовує цифрову трансформацію від технічного переоснащення. Водночас він недостатньо розкриває системний характер змін, не охоплює організаційну структуру, кадрові компетентності, управлінські механізми та зовнішню взаємодію організації.

- Мандич О., Бабко Н., Лишенко М., Харчевнікова Л. [26] вважають, що «цифрова трансформація - це впровадження сучасних технологій у бізнес-процеси підприємства, яке передбачає не лише встановлення сучасного обладнання, а й комплексну перебудову бізнес-моделі підприємства на основі цифрових інструментів» [26]. У визначенні цифрова трансформація пов'язується з упровадженням сучасних технологій і комплексною перебудовою бізнес-моделі підприємства. Сильною стороною є акцент на комплексності змін та їх поширенні на базову модель діяльності. Проте формулювання фактично починається з ототожнення цифрової трансформації з упровадженням технологій, що звужує її зміст і недостатньо відображає зміни у структурі, управлінні, взаємодії суб'єктів та організаційній культурі.

- Bouée C., Schaible S. [111] вказують, що «цифрова трансформація - послідовна мережа всіх секторів економіки та адаптацію гравців до нових реалій цифрової економіки. Рішення в мережевих системах включають обмін та аналіз даних, розрахунок та оцінку варіантів, а також ініціювання дій та впровадження наслідків» [111]. Автори розглядають цифрову трансформацію через мережеву інтеграцію секторів економіки, адаптацію учасників до цифрової економіки, обмін і аналіз даних та ініціювання відповідних дій. Перевагою є вихід за межі окремого підприємства та розуміння цифрової трансформації як міжсекторального й мережевого процесу. Водночас визначення має дещо описовий характер, не встановлює чітких меж поняття та змішує цифрову трансформацію з цифровою взаємодією, аналізом даних і адаптацією до цифрового середовища.

- Куйбіда В.С., Карпенко О.В., Наместнік В.В. [23] вважають, що «цифрові трансформації – спричинені використанням цифрових технологій зміни в природі людини, її мисленні, життєдіяльності та управлінні» [23]. Цифрові трансформації розглядаються як зміни в природі людини, її

мисленні, життєдіяльності та управлінні, спричинені цифровими технологіями. Цінність підходу полягає в його суспільній і державно-управлінській спрямованості, а також у визнанні того, що цифровізація змінює не лише технічні процеси, а й поведінку, мислення та моделі управління. Разом із тим визначення є надто широким і не конкретизує об'єкт, зміст, етапи, суб'єктів та цільові результати цифрової трансформації.

- Струтинська І.В. [69] пропонує розглядати цифрову трансформацію як «перехід на цифрові технології, орієнтованість на користувача. Поява нових інструментів взаємодії з клієнтом, таких як чат-боти, термінали самообслуговування або онлайн-кабінети, змінює споживчу поведінку. У широкому розумінні термін «цифрова трансформація» слід трактувати як незворотний процес впровадження цифрових технологій в умовах розвитку ери цифрової економіки для вдосконалення життєдіяльності людини, бізнесу, суспільства і держави загалом». Авторка поєднує вузьке розуміння цифрової трансформації як переходу на цифрові технології та орієнтації на користувача з широким трактуванням як незворотного процесу вдосконалення життєдіяльності людини, бізнесу, суспільства і держави. Перевагою є людиноцентричність і поширення поняття за межі підприємницької діяльності. Водночас ототожнення цифрової трансформації з переходом на цифрові технології звужує її до технологічного оновлення, а характеристика процесу як безумовно незворотного та спрямованого на вдосконалення не враховує можливих ризиків, негативних наслідків і неоднозначності результатів цифрових змін.

- Нікітін Ю.О. [209] вказує, що «цифрова трансформація – це процес переходу до нових способів діяльності підприємства шляхом впровадження цифрових технологій та цифрових сервісів, що базується на стратегічному партнерстві всіх зацікавлених сторін та одночасної розробки програмного забезпечення, цифрової трансформації та оцінки

рівня цифрової трансформації підприємства» [209]. Цифрова трансформація визначається як перехід підприємства до нових способів діяльності на основі цифрових технологій і сервісів, стратегічного партнерства заінтересованих сторін, розроблення програмного забезпечення та оцінювання рівня трансформації. Сильною стороною є включення взаємодії стейкхолдерів та оцінювання результатів, що наближає підхід до управлінського розуміння процесу. Проте дефініція є перевантаженою окремими інструментами реалізації, а згадування «розробки цифрової трансформації» створює понятійну нечіткість і не розкриває, які саме властивості об'єкта зазнають якісних змін.

Проведений аналіз свідчить, що поняття «цифрова трансформація» переважно сформувалося в межах економічних наук та управління підприємствами. Більшість авторів пов'язують його з упровадженням цифрових технологій, зміною бізнес-процесів, організаційних моделей, способів взаємодії зі споживачами та підвищенням результативності діяльності. Перевагою цих підходів є відмежування цифрової трансформації від звичайної автоматизації або технічного переоснащення, оскільки вона передбачає комплексні та якісні зміни об'єкта.

Водночас існуючі дефініції мають низку обмежень:

- по-перше, значна частина визначень звужує об'єкт трансформації до підприємства та його бізнес-моделі, що ускладнює їх застосування до держави, публічної сфери й складних соціальних систем.

- по-друге, цифрова трансформація нерідко ототожнюється із впровадженням цифрових технологій, хоча технології є лише засобом ініціювання змін, а не самим змістом трансформації.

- по-третє, недостатньо розкритими залишаються суб'єкти управління, цілі, механізми координації, ресурсне забезпечення, ризики та суспільні результати цифрових змін.

- по-четверте, у більшості підходів не показано, що цифрова трансформація змінює не лише процеси й технології, а й властивості, структуру, функції, взаємозв'язки та принципи функціонування об'єкта.

Для вирішення зазначених проблем та в контексті об'єктно-предметного поля даного дослідження, вважаємо, що цифрова трансформація - це 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.

Зазначений підхід має бути покладений в розуміння поняття цифрової трансформації системи охорони здоров'я. На державному рівні цифрова трансформація охорони здоров'я визначається через формування політичних, правових, організаційних, технологічних та інших умов розвитку електронної системи охорони здоров'я. Перевагою такого підходу є комплексне врахування державної політики, нормативно-правового забезпечення та організаційних передумов цифрової трансформації. Водночас основний акцент зроблено на створенні умов цифрового розвитку, а не на розкритті змісту цифрової трансформації як процесу якісної зміни системи охорони здоров'я [19].

Разом з тим, щодо змісту поняття цифрова трансформація системи охорони здоров'я в науковій літературі містяться наступні підходи:

- Agarwal R., Gao G., DesRoches C., Jha A.K. [86] вважають, що «цифрова трансформацію охорони здоров'я як масштабне впровадження інформаційних технологій (Health IT), спрямоване на підвищення безпеки, доступності та ефективності систем охорони здоров'я» [86]. Перевагою

підходу є визначення стратегічної мети цифрової трансформації через покращення результативності функціонування системи. Разом із тим цифрова трансформація фактично ототожнюється із впровадженням інформаційних технологій, що звужує її зміст та не враховує інституційні, організаційні, правові та управлінські зміни.

- Gopal G., Suter-Crazzolara C., Toldo L., Eberhardt W. [167] визначають цифрову трансформацію як процес створення комплексної інформаційної бази даних про здоров’я пацієнта та інтеграції сучасних цифрових технологій, зокрема Інтернету речей, машинного навчання, аналітики даних і штучного інтелекту. Позитивною рисою є акцент на інтеграції цифрових технологій та використанні медичних даних як основи цифрової медицини. Водночас цифрова трансформація розглядається переважно крізь призму інформаційно-технологічної інфраструктури, залишаючи поза увагою зміни у системі державного управління, організації медичної допомоги та взаємодії суб'єктів системи охорони здоров’я.

- Marques I.C., Ferreira J.J. [208] вказують, що «цифрова трансформація охорони здоров'я еволюційний процес запровадження цифрових технологій у клінічну практику й управління системою охорони здоров'я, що змінює взаємодію між пацієнтами, лікарями та постачальниками медичних послуг». Перевагою є розгляд цифрової трансформації як процесу зміни взаємодії між основними учасниками системи. Разом із тим визначення концентрується переважно на клінічній практиці та взаємодії учасників, не розкриваючи системних змін у структурі, функціях та механізмах функціонування системи охорони здоров'я.

- Мартиненко О.В., Малярова Л.В. [27] пропонують під цифровою трансформацією розуміти «процес запровадження електронної системи охорони здоров’я, реєстрів, телемедицини та інших інформаційно-комунікаційних систем, що ґрунтується на міжнародному досвіді та

ключових документах ВООЗ з цифровізації охорони здоров’я в Європейському регіоні» [27]. Перевагою є орієнтація на сучасні практичні інструменти цифровізації та міжнародні рекомендації ВООЗ. Разом із тим цифрова трансформація фактично ототожнюється з переліком цифрових технологій та інформаційних систем, що не дозволяє розкрити її як комплексний процес якісних змін системи охорони здоров'я.

- Бачук О.Р. [3] визначає цифрову трансформацію системи охорони здоров'я як комплексний організаційно-управлінський процес переходу закладів та органів управління до цифрових технологій обробки медичної інформації. Сильною стороною є розгляд цифрової трансформації саме як управлінського процесу та врахування ролі органів управління охороною здоров'я. Разом із тим основна увага приділяється цифровій обробці інформації, тоді як трансформація охоплює значно ширші зміни структури, процесів, моделей взаємодії, механізмів управління та властивостей системи.

Проведений аналіз свідчить, 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.

Разом із тим більшість наведених підходів не розкриває цифрову трансформацію системи охорони здоров'я як об'єкт державного управління. Поза увагою залишаються питання зміни властивостей системи охорони здоров'я, трансформації механізмів державного управління, розвитку інституційної взаємодії, організаційної структури,

кадрового потенціалу, ресурсного забезпечення, моделей надання медичних послуг та інформаційної взаємодії між усіма суб'єктами системи. Крім того, цифрова трансформація нерідко ототожнюється із впровадженням окремих цифрових технологій або інформаційних систем, хоча останні є лише інструментами досягнення якісно нового стану системи.

У зв'язку з цим виникає необхідність формування нового державно-управлінського підходу, відповідно до якого цифрова трансформація системи охорони здоров'я розглядається як комплексний, цілеспрямований і керований процес якісної зміни всієї системи охорони здоров'я, що охоплює її структуру, властивості, функції, процеси, механізми управління, взаємодію суб'єктів, ресурси та способи реалізації медичних послуг під впливом цифрових технологій.

Цифрова трансформація системи охорони здоров'я - це 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.

За результатами дослідження розширено теоретичне наукове значення державного управління через уточнення змісту понять та категорій, а саме: система охорони здоров'я (багаторівнева соціально-економічна 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 громадянського 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.)

Висновки до 1-го розділу

1. Систематизація факторів впливу засвідчує, що цифрова трансформація системи охорони здоров’я детермінується сукупністю зовнішніх суспільних викликів та внутрішніх інституційно-ресурсних спроможностей держави. 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.

2. 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 Європейського Союзу 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.

3. 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.

4. Бібліометричний аналіз публікацій у Scopus за запитом «digital healthcare systems» засвідчив стрімке зростання наукового інтересу до цієї тематики після 2020 року. 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.

5. 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. 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 громадянського 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.

6. 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).

РОЗДІЛ 2
МЕТОДОЛОГІЯ ДЕРЖАВНОГО УПРАВЛІННЯ ЦИФРОВОЮ ТРАНСФОРМАЦІЄЮ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я

2.1. Вплив цифрової трансформації на властивості системи охорони здоров'я та процес прийняття державно-управлінських рішень

Питання цифрової трансформації системи охорони здоров'я є досить складним процесом, адже охоплює як медичні, так і управлінські, соціальні, економічні та інші аспекти. Державне управління в даному процесі займає вагому роль, адже:

- по-перше, формує правове поле державного регулювання процесів цифровізації та застосування інформаційно-комунікаційних технологій в процесі реалізації медичних послуг та надання медичної допомоги;

- по-друге, формує та реалізовує сукупність заходів із забезпечення безпеки системи охорони здоров'я в умовах цифрових трансформацій та застосування технологій штучного інтелекту;

- по-третє, здійснює фінансування процесів цифрової трансформації системи охорони здоров'я;

- по-четверте, впроваджує інформаційно-комунікаційні технології в практику прийняття та реалізації державно-управлінських рішень.

«Цифровізація системи охорони здоров'я в сучасних умовах перетворилася на один із ключових напрямів трансформації медичної галузі, поєднуючи технологічні інновації, нові формати надання медичних послуг, зміну підходів до управління даними та фінансовими ресурсами. Актуальність аналізу світових тенденцій цифрової трансформації системи

охорони здоров’я зумовлена тим, що масштаби її поширення безпосередньо залежать від рівня розвитку медичної інфраструктури, доступності цифрових сервісів для населення, рівня його цифрової грамотності, спроможності систем охорони здоров’я працювати з великими масивами даних, а також від здатності держави забезпечувати кібербезпеку й належний захист персональної медичної інформації. У цьому контексті цифровізація охорони здоров’я не обмежується впровадженням нових технічних рішень, а охоплює комплекс управлінських, організаційних, соціальних і фінансових питань, пов’язаних із забезпеченням доступності, безпеки та результативності медичних послуг» [34].

Цифрова трансформація системи охорони здоров’я відбувається в декількох контекстах, зокрема:

- цифрова трансформація об’єкту державного управління, а саме реалізації медичних послуг та надання медичної допомоги усіх видів та рівнів, діяльності державних, комунальних та приватних закладів охорони здоров’я;

- цифрова трансформація діяльності суб’єктів державного управління системою охорони здоров’я як на рівні держави, так і на рівні регіону та місцевого самоврядування;

- цифрова трансформація управління організаційною, медичною, фінансовою діяльністю закладів охорони здоров’я усіх рівнів та усіх форм власності;

- цифрова трансформація медичної послуги, що полягає як в розвитку телемедицини, так і у використанні сучасних інформаційно-комунікаційних технологій в медицині на рівні діагностики, лікування, реабілітації та профілактики, в тому числі застосування технологій штучного інтелекту.

Питання зміни властивостей системи охорони здоров'я під впливом цифрової трансформації піднімали в наукових працях зарубіжних вчених, зокрема: Adler-Milstein J., Jha A.K., Agbo C.C., Mahmoud Q.H., Eklund J.M., Ashley E.A., Biancone P., Secinaro S., Marseglia R., Calandra D., Buntin M.B., Burke M.F., Hoaglin M.C., Blumenthal D., Char D.S., Shah N.H., Magnus D., Cresswell K.M., Worth A., Sheikh A., Dal Mas F., Massaro M., Rippa P., Secundo G., Dorsey E.R., Topol E.J., Free C., Phillips G., Watson L., Galli L., Felix L., Edwards P., Patel V., Haines A., Hsiao C.J., Hing E., Ashman J., Islam S.M.R., Kwak D., Kabir M.H., Hossain M., Kwak K.S., Koonin L.M., Hoots B., Tsang C.A., Leroy Z., Farris K., Jolly B., Antall P., McCabe B., Zelis C.B., Tong I., Harris A.M., Kruse C.S., Frederick B., Jacobson T., Monticone D.K., Kvedar J., Coye M. J., Everett W., Massaro M., Meskó B., Drobni Z., Bényei É., Gergely B., Győrffy Z., Raghupathi W., Raghupathi V., Raimo N., De Turi I., Albergo F., Vitolla F., Schallmo D., Williams C.A., Boardman L., Sims S., Reed J.E., Weaver T., Stoumpos A.I., Kitsios F., Talias M.A. та інші. Серед вітчизняних вчених питання цифрової трансформації системи охорони здоров'я досліджували представники різних галузей знань (економічні, технічні, медичні, юридичні, політичні, державно-управлінські науки): Бачук О.Р., Музика-Стефанчук О.А., Стефанчук М.О., Якимчук Н.Я., Руденко Р.І., Запорожець Т.В., Шлапко Т.В., Старинський М.В., Миргород-Карпова В.В., Опанасюк М.О., Криничко Л.Р., Мотайло О.В., Олійник М.О., Юнгер В.І., Грицишен Д.О., Антонова Л.В., Сергієнко Л.В., Драган І.В., Драган І.О., Ксендзук В.В., Петрик С.М., Курбанов А.К., Вакун О.В., Орлова Н.С. та інші.

«Сучасні виклики цифровізації охорони здоров'я мають не лише технічний, а й глибоко соціальний, комунікаційний та інституційний характер. Їх вирішення вимагає комплексного підходу: вдосконалення

стандартів взаємодії між державними та приватними компонентами eHealth, забезпечення цифрової інклюзії через освітні програми, зміцнення комунікаційних каналів та оновлення нормативно-правової бази з урахуванням потреб громадян та стейкхолдерів. Лише системна політика, заснована на прозорості, доступності та ефективності, дозволить досягти соціальної справедливості в процесі цифрової трансформації сфери охорони здоров'я» [79].

Державне управління в даному контексті виконує сукупність функцій та може розглядатися як об'єкт цифрової трансформації, так і як регулятор цифрової трансформації. Під впливом цифровізації відбувається трансформація властивостей як медичної послуги, так і властивостей державного управління системою охорони здоров'я. Причому дані властивості можуть нести в собі як переваги, так і ризики і загрози для суспільства, системи охорони здоров'я та окремої особи. Адже, як зазначають вітчизняні дослідники: «масштаби цифровізації охорони здоров'я не є тотожними рівню цифрової зрілості національних систем, оскільки між країнами та регіонами зберігаються суттєві відмінності у доступності цифрової інфраструктури, ступені інтероперабельності інформаційних систем, рівні цифрових компетентностей населення і медичних працівників, а також у спроможності забезпечувати пацієнтоцентричний доступ до медичних даних. Встановлено, що важливими обмежувальними чинниками залишаються фрагментарність електронних медичних записів, нерівномірність поширення телемедичних послуг, залежність від сторонніх постачальників цифрових рішень, а також наявність інфраструктурних, фінансових та нормативноорганізаційних перешкод. Обґрунтовано, що результативність цифрової трансформації охорони здоров'я визначається не лише темпами технологічного оновлення, а передусім здатністю держави забезпечити узгодженість між

політикою управління даними, механізмами фінансування, нормативно-правовим регулюванням, розвитком цифрових компетентностей і формуванням суспільної довіри до цифрових медичних сервісів» [34].

В науковій літературі не існує єдиних підходів до складу та змісту властивостей системи охорони здоров'я. В окремих дослідженнях вчені виділяли сукупність властивостей системи охорони здоров'я, в контексті досягнення певних цілей, що обумовлені стратегіями, програмами, реформами.

Вітчизняний вчений Курбанов А.К. при вивченні проблем державного управління потенціалом системи охорони здоров'я вказує на її наступні властивості:

«- міжгалузевість: система охорони здоров'я поєднує в собі сукупність галузей національної економіки як в сфері послуг, так і в сфері товарів та робіт. Так, власне, система охорони здоров'я націлена на реалізацію медичних послуг через надання медичної допомоги різних рівнів з одного боку та формування сукупності профілактичних заходів для зміцнення здоров'я населення – з іншого. Важливе значення у функціонуванні системи охорони здоров'я займають послуги з обслуговування інфраструктури, які не пов'язані із реалізацією медичних послуг (водопостачання, енергопостачання, газопостачання, харчування та інші). Матеріальне забезпечення здебільшого складається із постачання ліків та медичного обладнання та технологій.

- професійність: система охорони здоров'я залежить від кадрового потенціалу, адже значною мірою ефективність, своєчасність, якість, результативність медичних послуг залежить від професійності та компетентності лікаря. Відповідно на систему охорони здоров'я покладається підготовка та перепідготовка медичних та управлінських кадрів, що здійснюється як через відомчі, так і через інші заклади вищої

освіти. Це і складає кадровий потенціал системи охорони здоров'я, що безумовно визначає можливість в повній мірі реалізовувати завдання, які покладаються на систему охорони здоров'я.

- динамічність: система охорони здоров'я є динамічною системою, яка характеризується залежністю від сукупності внутрішніх та зовнішніх факторів. Внутрішні фактори визначаються розвитком медичних технологій, нових методів лікування та станом здоров'я населення. Зовнішні фактори характеризуються екологічними, політичними, економічними та іншими чинниками, які впливають як власне на громадське здоров'я населення, так і на систему охорони здоров'я загалом.

- соціальність: система охорони здоров'я є соціальною сферою, адже має забезпечити високий рівень задоволеності населення медичними послугами та відповідний рівень громадського здоров'я населення. Адже, переслідує ключову мету – забезпечення громадського здоров'я населення в цілому та здоров'я окремої особи зокрема. Стан громадського здоров'я важливо розглядати крізь призму управління потенціалом, адже здорове населення характеризує потенціал людського капіталу для економіки держави з одного боку та вивільняє ресурси охорони здоров'я для забезпечення розвитку її інноваційного потенціалу – з іншого.

- високий рівень заінтересованості: система охорони здоров'я є складовою реалізації соціальної функції держави та завжди знаходиться на перетині приватних, суспільних та державних інтересів. У високому рівні охорони здоров'я зацікавлені як громадяни, так і держава з бізнесом. Водночас, функціонування системи охорони здоров'я пов'язане із ресурсним забезпеченням, а отже взаємодією із бізнесом у фармацевтичній, технологічній, освітній, обслуговуючій сферах.

- наукоємна: система охорони здоров'я є прямо залежною від розвитку науки як медичної так і технічної, фармацевтичної, економічної та інших. Система охорони здоров'я має розвиватися в контексті медичної науки,

адже запровадження нових методів лікування є основою високого рівня ефективності та якості медичних послуг та відповідно результативності усієї системи охорони здоров'я. Фармацевтична наука розвивається в напрямку підвищення ефективності існуючих ліків та розробки нових, тому саме на цьому має базуватися розвиток системи охорони здоров'я.

- багаторівнева: система охорони здоров'я характеризується як багаторівнева соціальна система, що проявляється як в рівнях державного управління системою охорони здоров'я, так і в рівнях медичних послуг. Відповідно потенціал системи охорони здоров'я варто також розглядати на різних рівнях» [24].

Юнгер В.І. при вивченні проблем повоєнного відновлення системи охорони здоров'я вказує, що нова система охорони здоров'я має бути наділена трьома властивостями:

«- адаптивність: можливість якісно та оперативно надавати медичні послуги цивільному населенню в умовах надзвичайних ситуацій; можливість оперативно змінювати діяльність закладів охорони здоров'я для надання медичних послуг військовим; можливість забезпечення евакуації закладів охорони здоров'я з територій надзвичайних ситуацій, зокрема бойових дій.

- стійкість: можливість швидкого відновлення системи охорони здоров'я в цілому та окремих складових внаслідок надзвичайних ситуацій; можливість швидкої релокації закладів охорони здоров'я.

- безпечність: забезпечення безперебійної роботи закладів охорони здоров'я в умовах надзвичайних ситуацій; забезпечення безпеки медичного персоналу та пацієнтів в умовах надзвичайних ситуацій; можливість безперебійної ізольованої роботи закладу охорони здоров'я певний проміжок часу» [78].

Криничко Л.Р. пропонує виділяти лише три властивості системи охорони здоров’я, зокрема:

1) стейкхолдери: зацікавленість більшості суб’єктів соціально-економічних відносин та суб’єктів державного управління в розвитку системи охорони здоров’я як фактору формування людського капіталу держави, що є основою розвитку інших соціально-економічних систем;

2) багатогалузевість: система охорони здоров’я включає в себе сукупність галузей економіки як власне надання медичних послуг, так і фармацевтичну галузь, галузь з виробництва медичних технологій; систему освіти медичних працівників тощо;

3) взаємозалежність: система охорони здоров’я взаємопов’язана із соціально-економічними та політичними системами та природно-кліматичними умовами» [21].

Зазначені підходи характеризували систему охорони здоров’я лише з позиції об’єктно-предметного поля дослідження вчених, а також мети їх наукового пошуку. Вважаємо, що властивості системи охорони здоров’я варто досліджувати за наступними напрямками:

1. Властивості, які характеризують систему охорони здоров’я як систему соціально-економічних відносин. Такими властивостями є наступні, що в свою чергу піддаються змінам в умовах цифровізації:

- відкритість (взаємодія із зовнішнім середовищем, що визначає систему охорони здоров’я залежну від соціально-економічного, політико-правового, техніко-технологічного розвитку суспільства). Цифровізація підвищує відкритість системи охорони здоров'я шляхом розширення інформаційної взаємодії із зовнішнім середовищем, забезпечення інтеграції з національними та міжнародними цифровими платформами, оперативного обміну даними та швидкого впровадження технологічних і нормативних змін.

- ієрархічність (багаторівнева структура системи та управління її функціонуванням, що визначає багатовекторність та багаторівневість системи охорони здоров’я як з позиції реалізації медичних послуг (надання медичної допомоги) так і з позиції управління нею (на рівні держави, регіону, територіальної громади та закладу охорони здоров’я)). Цифровізація видозмінює ієрархічність системи охорони здоров'я шляхом інтеграції цифрових інформаційних систем між усіма рівнями її функціонування, забезпечуючи безперервний обмін даними, координацію процесів надання медичної допомоги та узгодженість управлінських рішень від закладу охорони здоров'я до державного рівня. В той же час варто зазначити, що цифровізація не стільки посилює ієрархічність, скільки оптимізує її реалізацію. Ієрархічність є структурною властивістю системи, яка існує незалежно від цифрових технологій, а цифровізація робить взаємодію між рівнями швидшою, прозорішою та більш інтегрованою.

- керованість (визначає можливість управління системою, тобто характеризує систему охорони здоров’я як об’єкт державного управління (за різними рівнями державний, регіональний, територіальної громади)). Цифровізація підвищує рівень керованості системи охорони здоров'я завдяки формуванню єдиного цифрового інформаційного простору, який забезпечує ефективну координацію, моніторинг, контроль і підтримку прийняття управлінських рішень на всіх рівнях функціонування системи.

- інтегрованість (узгодженість функціонування усіх елементів системи, що визначає взаємодію між різними рівнями надання медичної допомоги). Цифровізація забезпечує інтегрованість системи охорони здоров'я шляхом забезпечення безперервного обміну медичними даними, інформаційної взаємодії між усіма рівнями надання медичної допомоги та узгодженості клінічних і організаційних процесів.

- координованість (взаємодія між суб’єктами системи, що характеризує систему охорони здоров’я з позиції взаємодії між закладами охорони здоров’я та суб’єктами державного, регіонального та територіального управління). Цифровізація підвищує координованість системи охорони здоров'я, забезпечуючи своєчасний обмін інформацією, узгодження дій та ефективну взаємодію між закладами охорони здоров'я і суб'єктами управління різних рівнів.

- підзвітність (відповідальність за результати діяльності, так кожен елемент системи охорони здоров’я є підзвітний державі або місцевому самоврядуванню, крім того, заклад охорони здоров’я має також певний рівень підзвітності). Цифровізація забезпечує прозорий облік діяльності, простежуваність процесів, автоматизований моніторинг результатів та оперативний контроль за виконанням повноважень усіма суб'єктами системи.

- багатогалузевість - властивість системи охорони здоров'я інтегрувати діяльність різних галузей економіки та суспільної сфери, зокрема медичної, фармацевтичної, наукової, освітньої, біотехнологічної, інформаційно-комунікаційної, логістичної та виробничої, які спільно забезпечують надання медичної допомоги та функціонування системи. Цифровізація удосконалює окремі галузі, а також посилює взаємодію між ними, забезпечуючи цифрову інтеграцію, безперервний обмін даними та ефективну взаємодію між медичною, фармацевтичною, науковою, освітньою, біотехнологічною, інформаційно-комунікаційною, логістичною та виробничою сферами.

- наукоємність (залежність від розвитку науки, що характеризує систему охорони здоров’я як систему, що потребує постійного наукового супроводу для удосконалення процесів лікування, медичних технологій, управління та інших процесів, що пов’язані із реалізацією медичних або суміжних послуг). Цифровізація прискорює впровадження результатів наукових досліджень у систему охорони здоров'я, забезпечуючи

використання цифрових технологій, аналітики даних та штучного інтелекту для вдосконалення медичних технологій, клінічної практики й організації медичної допомоги.

- соціальність - властивість системи охорони здоров'я забезпечувати реалізацію суспільно значущих потреб у сфері охорони здоров'я, сприяти підвищенню якості життя населення та покращенню показників громадського здоров'я. Цифровізація розширює можливості системи охорони здоров'я щодо задоволення суспільно значущих потреб шляхом підвищення доступності, своєчасності, персоналізації та безперервності надання медичної допомоги, що сприяє покращенню рівня громадського здоров'я.

- професійність (характеризує залежність системи охорони здоров’я від професійності медичного, управлінського, допоміжного та іншого персоналу). Цифровізація трансформує професійність персоналу системи охорони здоров'я, зумовлюючи необхідність розвитку цифрових компетентностей, безперервного професійного навчання та ефективного використання сучасних цифрових технологій у професійній діяльності.

Зазначені властивості характеризують систему охорони здоров’я як динамічну керовану систему суспільних відносин, що полягає в забезпеченні реалізації соціальної функції держави, що направлена на збереження здоров’я людини та забезпечення високого рівня громадського здоров’я. Цифрова трансформація дозволяє трансформувати зазначені властивості, що впливають як на їх зміст, так і на реалізацію завдань системи охорони здоров’я. Відповідно державне управління системою охорони здоров’я має сукупність видозмінених завдань, які з одного боку спрощують процеси прийняття та реалізації державно-управлінських рішень, а з іншого вимагають трансформації безпекових та правових інструментів, особливо в частині забезпечення кіберзахистув частині та використання технологій штучного інтелекту.

2. Властивості, які характеризують розвиток системи охорони здоров’я та задоволеність стейкхолдерів її функціонуванням:

- цілісність та комплексність – функціонування системи охорони здоров’я як єдиної системи, що передбачає ефективну систему взаємодії, комунікації та реагування елементів системи на зміни у внутрішньому та зовнішньому середовищі, для забезпечення функціонування усіх елементів системи як єдиного комплексного організму. Цифровізація забезпечує цілісність і комплексність функціонування системи охорони здоров'я шляхом інтеграції інформаційних ресурсів, цифрових сервісів і процесів, створюючи єдиний інформаційний простір для ефективної взаємодії, комунікації та узгодженого реагування всіх її елементів на внутрішні й зовнішні зміни.

- адаптивність та стійкість – передбачає управління системою охорони здоров’я таким чином, щоб забезпечити її функціонування (реалізацію медичних послуг) під впливом внутрішніх та зовнішніх факторів та сформувати здатність пристосовуватися до змін, таким чином, щоб виконувати покладені завдання. Цифровізація забезпечує адаптивність і стійкість системи охорони здоров'я шляхом оперативного моніторингу, прогнозування, аналізу даних та підтримки своєчасного прийняття рішень, що дозволяє ефективно реагувати на внутрішні й зовнішні виклики та забезпечувати безперервність надання медичної допомоги.

- безперервність та доступність – властивість системи охорони здоров’я, яка характеризує її можливість реалізації медичних послуг та забезпечення доступу до них населення за будь-яких умов внутрішнього та зовнішнього середовища. Цифровізація створює умови для забезпечення безперервності та доступності медичної допомоги шляхом впровадження цифрових технологій, що мінімізують територіальні, часові та організаційні бар'єри доступу до медичних послуг і підтримують їх надання в умовах внутрішніх та зовнішніх викликів. «Медицина трансформується: періодична діагностика стає онлайн-

діагностикою, Інтернет речей дозволяє за допомогою датчиків та сенсорів здійснювати постійний моніторинг стану здоров’я людини, оператори медичних і супутніх послуг та інфраструктури стають учасниками цифрових платформ – усе це впливає на якість, ефективність та функціональність системи медичної допомоги та супроводу громадян» [31]. Руденко Р.І. наголошує, що «реалізація сукупності механізмів публічного управління (нормативноправових, організаційно-координаційних, інформаційних та аналітичних) забезпечила підвищення доступності медичних послуг, безперервності функціонування медичної системи, ефективності використання ресурсів а також надання безпечної медичної допомоги в умовах воєнного стану. Зазначене підтверджує сприйняття на даний час цифрових трансформацій як повноцінного механізму реалізації публічної політики, спрямованої на забезпечення якості життя населення» [63].

- якість та ефективність – досягнення відповідного рівня медичних послуг, що забезпечує високий рівень громадського здоров’я, шляхом раціонального використання ресурсів (державних, приватних, міжнародних). Цифровізація сприяє досягненню вищого рівня якості та ефективності системи охорони здоров'я завдяки інформаційній підтримці клінічних і управлінських рішень, оптимізації використання ресурсів та впровадженню цифрових технологій у процеси надання медичної допомоги.

- безпечність - властивість системи охорони здоров'я забезпечувати надання медичної допомоги з мінімізацією ризиків для життя і здоров'я пацієнтів, медичних працівників та інших учасників медичного процесу, а також запобігати виникненню медичних помилок, інфекцій, несприятливих подій та інших загроз для елементів системи охорони здоров’я, зокрема закладів охорони здоров’я. Цифровізація мінімізує ризики під час надання медичної допомоги шляхом використання цифрових технологій моніторингу, підтримки клінічних рішень, автоматизованого контролю медичних процесів

та інформаційного супроводу, що сприяє запобіганню медичним помилкам, несприятливим подіям і загрозам для пацієнтів, медичних працівників та закладів охорони здоров'я.

- прозорість - властивість системи охорони здоров'я забезпечувати відкритість, зрозумілість і доступність інформації про організацію, функціонування, порядок надання медичної допомоги, використання ресурсів та прийняття рішень для всіх заінтересованих сторін. Цифровізація забезпечує відкритість, простежуваність і доступність інформації про функціонування системи охорони здоров'я завдяки впровадженню цифрових інформаційних систем та електронних сервісів.

Представлений склад властивостей системи охорони здоров’я вказує на характеристики стану його розвитку та рівня реалізації завдань системи охорони здоров’я. Беззаперечно, що будь-якій системі охорони здоров’я характерні зазначені властивості, проте розвинена система має відповідний рівень вказаних властивостей.

3. Цифрова трансформація системи охорони здоров’я також дозволяє говорити про нові її властивості, які визначають сукупність переваг зокрема:

- інтероперабельність - властивість цифровізованої системи охорони здоров'я забезпечувати сумісність, безпечний обмін, спільне використання та однозначну інтерпретацію медичних даних між інформаційними системами, цифровими платформами й суб'єктами системи охорони здоров'я незалежно від їх організаційної чи технологічної належності;

- простежуваність - властивість цифровізованої системи охорони здоров'я забезпечувати можливість ідентифікації, відстеження та документування всіх етапів надання медичної допомоги, обігу медичних даних, використання ресурсів і прийняття рішень протягом усього життєвого циклу медичної послуги;

- автоматизованість - властивість цифровізованої системи охорони здоров'я забезпечувати автоматичне виконання, супровід і контроль окремих клінічних, діагностичних, адміністративних та інформаційних процесів із використанням цифрових технологій без необхідності постійного втручання людини. «Цифрова медицина повинна забезпечувати взаємодію між пацієнтами, медичними працівниками та установами за допомогою інформаційно-комунікаційних та цифрових технологій. Перехід медичного документообігу в електронний формат – одне з головних завдань цифрової медицини. Створення повноцінної цифрової медичної платформи є важливим кроком до цифровізації медичних та супутніх послуг, а також взаємодії операторів цієї сфери. Цифрова медична платформа – це динамічний набір систематизованих електронних даних про стан здоров’я окремого пацієнта, що забезпечує інформаційний обмін між учасниками процесу виробництва та споживання медичних послуг.»

- інтелектуальність - властивість цифровізованої системи охорони здоров'я використовувати технології штучного інтелекту, машинного навчання, аналітики даних та систем підтримки прийняття рішень для прогнозування, оптимізації й персоналізації процесів надання медичної допомоги. «У перспективі цифрові технології мають можливість значно посприяти розвитку сфери охорони здоров’я. Наприклад, штучний інтелект за секунди може аналізувати дані з усього світу і встановити діагноз по симптомам, який фахівець, що вперше з ним зіткнувся, може не розпізнати. В даному контексті не мається на увазі повна заміна людського ресурсу на штучний інтелект, проте потрібно розглянути перспективи цього напрямку з метою сприяння та допомоги фахівцям на основі комплексного використання діагностичного потенціалу сучасних технологій розробляти та використовувати безпечні протоколи конструювання індивідуальних реабілітаційних планів пацієнтів. А для проведення таких прогресивних

заходів цифрової трансформації навчання та підвищення кваліфікації осіб в межах кадрового забезпечення регіонів є вкрай необхідним» [77]. «З метою задоволення потреб пацієнта та лікаря медичної установи та створення електронної системи взаємозв'язку більш надійною і легшою для підтримки та використання слід чітко визначати необхідний функціонал системи для її належного застосування, уникаючи обширного функціоналу, що може бути зайвим для деяких користувачів та несе зайве навантаження на систему. Важливою функцією електронних систем взаємозв'язку пацієнта та лікаря є їх інтелектуалізація з метою прийняття оптимальних та ефективних рішень, тобто у процесі взаємодії з системою особа може прийняти, відкинути або на свій розсуд скоригувати запропоноване системою рішення, а отже, у такий спосіб відповідальність за прийняття рішення завжди покладається на конкретну особу – користувача» [77].

- прогностичність - властивість цифровізованої системи охорони здоров'я здійснювати прогнозування індивідуальних і популяційних медичних ризиків, потреб у медичних послугах, розвитку захворюваності та функціонування системи шляхом використання аналітики даних, математичного моделювання і технологій штучного інтелекту.

- просторова незалежність - властивість цифровізованої системи охорони здоров'я забезпечувати надання медичної допомоги, професійну взаємодію та обмін медичною інформацією незалежно від територіального розташування пацієнтів, медичних працівників і закладів охорони здоров'я. «Важливим елементом розбудови цифрової медицини є впровадження телесистем для надання дистанційних медичних послуг громадянам та підтримки роботи лікарів, особливо в сільській місцевості» [31]. «Ще одним важливим аспектом діджиталізації є телемедицина. Вона стрімко набирає популярність по всьому світу та дозволяє пацієнтам перебувати на зв'язку з лікарем регулярно, незалежно від власного

знаходження, особливо, це важливо для осіб з інвалідністю або ж для пацієнтів, які обстежуються та спостерігаються у закордонного лікаря. Важливо, що телемедицина вигідна і пацієнтам, і лікарям, адже перші можуть отримати консультацію стосовно свого стану здоров'я від лікарів з різних куточків світу, а другі матимуть можливість радитись та коллективно вирішувати подальші шляхи вирішення проблем пацієнта. Це вплине на медицину найкращим чином. Як приклад можна вказати Німеччину, де активно просувається телемедецина, і після її запровадження активно використовується громадянами» [77].

- масштабованість - властивість цифровізованої системи охорони здоров'я забезпечувати розширення функціональних можливостей, обсягів обробки медичних даних, кількості користувачів і цифрових сервісів без суттєвого зниження ефективності, якості та безпечності її функціонування.

Такі властивості в більшій мірі характеризуютьу більшій мірі переваги цифрової трансформації для системи охорони здоров'я, що визначаються як нові властивості з одного боку та дозволяють підвищити рівень властивостей, які характеризують рівень розвитку системи охорони здоров'я. Фактично такі властивості характеризують цілі державного управління цифровою трансформацією.

4. В той же час цифрова трансформація визначає інші властивості, які характеризують ризики та загрози для системи охорони здоров'я, зокрема:

- кіберзалежність - властивість цифровізованої системи охорони здоров'я, що характеризує її залежність від безпечного, безперервного та стабільного функціонування цифрової інфраструктури, інформаційно-комунікаційних систем і мереж, порушення роботи яких унаслідок кіберінцидентів або кібератак може призвести до зниження якості, доступності, безперервності чи безпечності надання медичної допомоги.

«Не менш активно розвивається напрям досліджень, присвячений кібербезпеці й штучному інтелекту в охороні здоров’я. ENISA зараховує сферу охорони здоров’я до найбільш уразливих до кібератак секторів, а серед основних загроз виокремлює програми-вимагачі, атаки на доступність сервісів та витоки даних. У відповідь на це ЄС у 2025 р. запропонував окремий план дій із кібербезпеки лікарень та медичних працівників. Паралельно ВООЗ у 2024–2025 рр. розгорнула нормативно-етичний напрям досліджень щодо застосування великих мультимодальних моделей у медицині, наголошуючи на необхідності прозорості, підзвітності, захисту приватності та людського контролю» [34].

- інформаційна залежність - властивість цифровізованої системи охорони здоров'я, що відображає ступінь залежності її функціонування від якості та доступності медичної інформації, порушення цілісності, достовірності чи доступності якої створює ризики для надання медичної допомоги, прийняття рішень і забезпечення безперервного функціонування системи;

- технологічна залежність - властивість цифровізованої системи охорони здоров'я, що характеризує її залежність від функціонування цифрових технологій, програмного забезпечення, технічних засобів і цифрової інфраструктури, порушення працездатності яких може негативно вплинути на надання медичної допомоги, обіг медичних даних та функціонування системи загалом.

- інфраструктурна залежність - властивість цифровізованої системи охорони здоров'я, що характеризує її залежність від безперебійного функціонування цифрової, телекомунікаційної та інженерної інфраструктури, порушення роботи якої може призвести до обмеження доступності цифрових сервісів, порушення обігу медичних даних і безперервності надання медичної допомоги.

- правова залежність - властивість цифровізованої системи охорони здоров'я, що характеризує її залежність від нормативно-правового регулювання цифрових технологій, обігу медичних даних, електронної взаємодії, кібербезпеки, використання систем штучного інтелекту та інших правових механізмів, які визначають умови функціонування, розвитку й застосування цифрових сервісів у сфері охорони здоров'я. «Для запровадження та прискорення діджиталізації в Україні необхідно удосконалити її правове забезпечення з урахуванням того, що насамперед мають створюватися такі бази даних та системи, що будуть стійкими до будь-яких випадкових негараздів або умисних злочинних дій. Для вдалого процесу діджиталізації необхідно забезпечити реалізацію наступних заходів: розрізнення медичних та персональних даних задля уникнення їх ідентифікації; відсутність накопичення в системі критичного обсягу персональних медичних даних задля уникнення їх несанкціонованого вилучення та використання; надання доступу користувачам лише до тієї інформації, яка може бути їм корисна та необхідна за функціональними обов’язками, з покладенням на кожного самостійної відповідальності за таку інформацію» [77].

Зазначені властивості-ризики мають бути враховані при формуванні та реалізації державно-управлінських рішень, для забезпечення ефективності процесів цифрової трансформації. В той же час увесь перелік властивостей піддається трансформації, адже цифрова трансформація ставить систему охорони здоров’я в сукупність залежностей технічного, технологічного та правового характеру. В той же час процеси цифрової трансформації вимагають посилення фінансового, правового, організаційного та інформаційного механізмів державного управління.

Структурування зазначених властивостей представлено на рисунку 2.1.

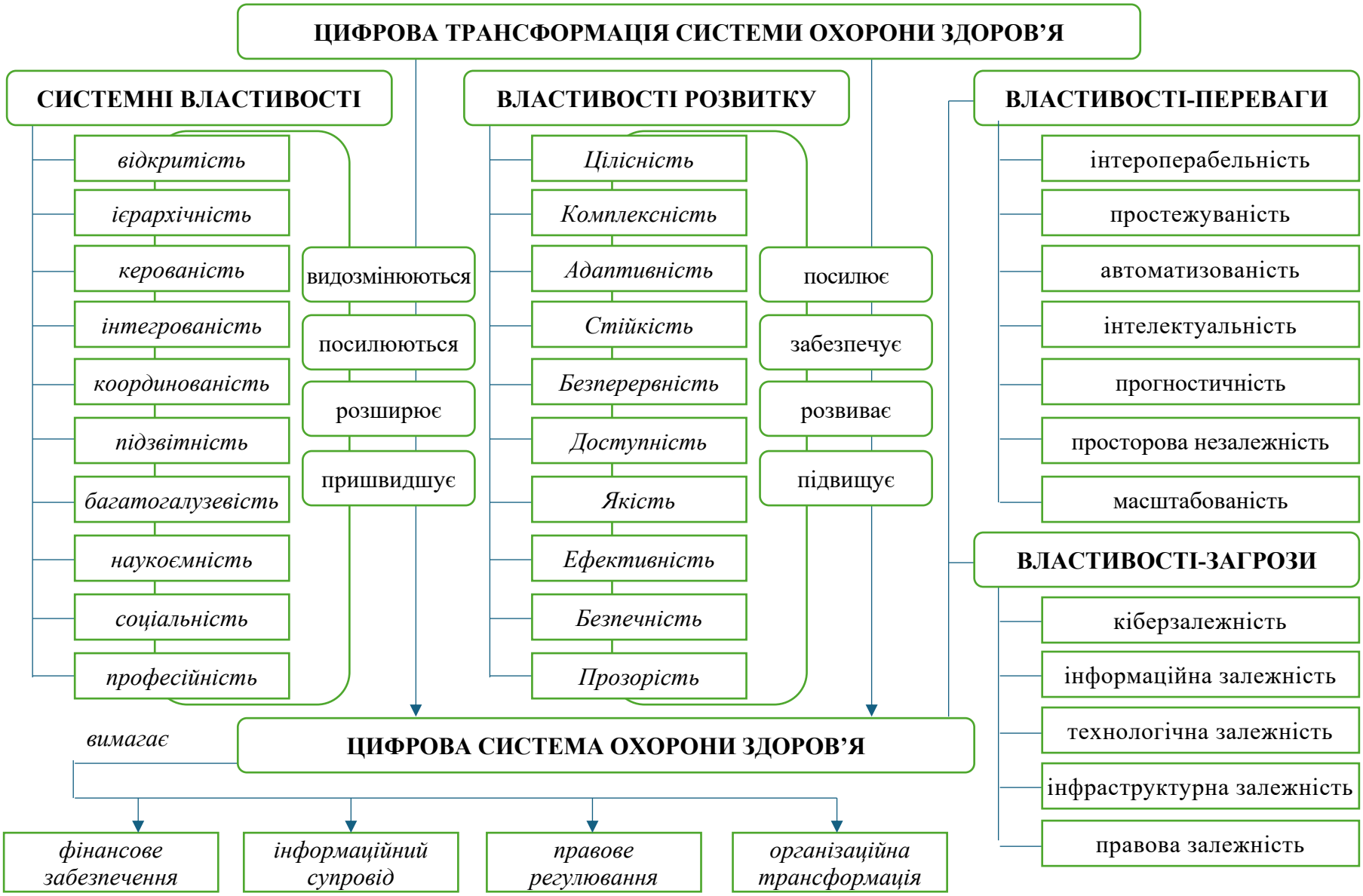

ЦИФРОВА ТРАНСФОРМАЦІЯ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я
СИСТЕМНІ ВЛАСТИВОСТІ
відкритість
ієрархічність
керованість
інтегрованість
координованість
підзвітність
багатогалузевість
наукоємність
соціальність
професійність
видозмінюються
посилюються
розширює
пришвидшує
ВЛАСТИВОСТІ РОЗВИТКУ
Цілісність
Комплексність
Адаптивність
Стійкість
Безперервність
Доступність
Якість
Ефективність
Безпечність
Прозорість
посилює
забезпечує
розвиває
підвищує
ВЛАСТИВОСТІ-ПЕРЕВАГИ
інтероперабельність
простежуваність
автоматизованість
інтелектуальність
прогностичність
просторова незалежність
масштабованість
ВЛАСТИВОСТІ-ЗАГРОЗИ
кіберзалежність
інформаційна залежність
технологічна залежність
інфраструктурна залежність
правова залежність
вимагає
ЦИФРОВА СИСТЕМА ОХОРОНИ ЗДОРОВ'Я
фінансове забезпечення
інформаційний супровід
правове регулювання
організаційна трансформація

Рис. 2.1. Властивості системи охорони здоров’я в умовах цифрової трансформації

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. 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. Визначені та згруповані властивості системи охорони здоров’я розширюють теоретичне наукове знання та формують методологічне підґрунтя державного управління цифровою трансформацією системи охорони здоров’я.

2.2. Принципи державного управління цифровою трансформацією системи охорони здоров'я.

Принципи державного управління та державної політики в сфері охорони здоров'я мають базуватися на властивостях об'єкту державно-управлінського впливу та формувати цілісне уявлення про методологію прийняття державно-управлінських рішень щодо цифрової трансформації системи охорони здоров'я. В науковій літературі питанню принципів державного управління системою охорони здоров'я присвячено багато підходів, які визначають їх склад та зміст. Безумовно, що дане питання є вкрай важливим з позиції. В цілому проаналізувавши наукову літературу можна виділити два фундаментальних напрямки дослідження принципів державного управління та державної політики в сфері охорони здоров'я: 1) характеризується виділенням системи принципів, за якими функціонує система державного управління в досліджуваній сфері в цілому; 2) виділення принципів за окремими складовими державного управління, зазвичай механізмами.

Перший напрямок характеризується визначенням складу та змісту принципів державного управління системою охорони здоров'я як цілісної системи, що в загальному визначається теоретико-методологічними положеннями державного управління з врахуванням галузевої специфіки.

Досить цікавим щодо групування та змісту принципів державного управління системою охорони здоров'я є підхід, що міститься в докторській дисертації Васюк Н.О. [4]. Так, вчена пропонує виділяти наступні групи принципів:

1. Принципи системного підходу в реалізації державної політики в сфері охорони здоров'я:

- багатомірності через врахування великої кількості властивостей сфери охорони здоров'я, які можуть бути об'єднані в групи або кластери для опису різних його особливостей;

- багатоплановості, який передбачає аналіз об'єкта (сфери охорони здоров'я) у різних аспектах, враховуючи його багатогранність;

- ієрархічності як базування на уявленні про ієрархічність структури системи та її властивостей, ранжування елементів у порядку від вищого до нижчого рівня;

- різнопорядковості властивостей, який ґрунтується на розумінні того, що закономірності можуть бути різного порядку і можуть бути властиві або усій системі, або лише окремим її рівням чи елементам;

- динамічності як розвиток сфери охорони здоров’я на усіх етапах суспільного розвитку з урахуванням динаміки та змін у часі.

2. Принципи інституційного підходу в реалізації державної політики в сфері охорони здоров’я:

- інституційної стабільності як забезпечення стійкості інституційних структур, що визначають правила гри в системі охорони здоров'я, сприяє ефективності та прогнозуванню довгострокових результатів;

- прозорості і відповідальності, що передбачає забезпечення чіткості та відкритості у взаємодії між інституціями, громадянами та іншими учасниками системи, а також визначення відповідальності за реалізацію державно-управлінських рішень;

- участі громадян шляхом залучення їх до процесу прийняття рішень та оцінки якості охорони здоров'я, що сприяє створенню більш ефективної та відповідальної системи;

- гнучкості та адаптивності як здатності інституційної системи відповідати на зміни у соціальному, економічному та технологічному середовищі для підтримки актуальних потреб у сфері охорони здоров'я;

- системної інтеграції, що пов’язується із забезпеченням співпраці між різними інституційними елементами, такими як медичні установи, фінансові структури та урядові органи, для досягнення цільових результатів, які визначені у стратегічних документах.

3. Принципи економічного підходу в реалізації державної політики в сфері охорони здоров’я:

- ефективність ресурсів як максимізація використання обмежених ресурсів з метою досягнення максимальної користі для громадян та системи охорони здоров'я;

- конкуренція та регулювання шляхом створення конкурентного середовища для стимулювання якості та ефективності медичних послуг та забезпечення їх доступності;

- ринкові механізми, які передбачають застосування принципів ринкової економіки для стимулювання інновацій, конкуренції та ефективності в системі охорони здоров'я;

- фінансова стійкість як умова забезпечення стабільного фінансування та запобігання кризам;

- залучення приватного сектору через політику сприяння участі приватних компаній та партнерств у наданні медичних послуг та інфраструктурному розвитку;

- фінансове заохочення для стимулювання досягнення конкретних цілей та покращення якості послуг;

- ефективні моделі страхування та фінансування для забезпечення доступності та якості медичних послуг.

4. Принципи соціального підходу в реалізації державної політики в сфері охорони здоров’я:

- соціальної справедливості як забезпечення рівних можливостей доступу до медичних послуг та ресурсів для всіх верств суспільства;

- соціальної відповідальності з акцентом на відповідальності суспільства за забезпечення загального благополуччя та підтримку осіб, які потребують медичної допомоги;

- емпатії та гуманізації, який реалізується шляхом врахування гуманітарних аспектів в наданні медичних послуг та створення людиноцентричних та пацієнтоорієнтованих підходів;

- соціокультурного контексту, який при формуванні та реалізації політики пов’язується із врахуванням культурних, етнічних та соціальних особливостей суспільства;

- прозорості та участі у виборі стратегій, активна участь громадян у прийнятті рішень та визначенні пріоритетів в охороні здоров'я;

- партнерства через залучення різних суб'єктів, таких як громадяни, бізнес, наука, до співпраці для досягнення спільних цілей у покращенні системи охорони здоров’я.

5. Принципи соціального підходу в реалізації державної політики в сфері охорони здоров’я:

- чітке визначення функцій шляхом визначення конкретних завдань та ролей, які виконує система охорони здоров'я в суспільстві, зокрема, надання медичних послуг, профілактики захворювань, реабілітації тощо;

- координованість між різними ланками системи охорони здоров'я для досягнення спільних цілей та оптимізації ресурсів;

- орієнтація на результати та встановлення чітких критеріїв результативності для оцінки досягнень системи охорони здоров'я та вимірювання її впливу на стан здоров’я населення;

- інтеграція з іншими секторами та іншими галузями, такими як освіта, соціальний захист, економіка, для комплексного підходу до проблем здоров'я;

- партисипація через залучення громади до процесів управління та реалізації політики з метою врахування їхніх потреб;

- комплексний підхід до здоров'я як комплексного явища, що включає фізичне, психічне, соціальне та економічне благополуччя населення;

- міжнародна співпраця як взаємодія та обмін інформацією, ресурсами та технологіями між різними країнами з метою поліпшення глобального здоров'я та вирішення спільних викликів у галузі.

Авторський підхід у більшій мірі характеризує не принципи державного управління системою охорони здоров’я, а визначає принципи застосування різних підходів до вивчення державного управління системою охорони здоров’я. Їх застосування є цілком логічним при дослідженні державного управління як комплексного об’єкту наукового пошуку.

Пазєєва Г. пропонує виділяти загальні та специфічні принципи управління закладом охорони здоров’я, зазначаючи їх наступний склад:

«- загальні принципи управління: цілеспрямованості, науковості, об’єктивності, гнучкості, безперервності, оперативності, оптимальності, економічної доцільності, єдиноначальності, достатність у централізації та децентралізації управління, делегування повноважень, ефективність;

- специфічні принципи управління: системність, безпека надання медичної допомоги, конституційність прав споживачів, достатність ресурсів, наявність перспективи, використання, взаємозалежність, динамічна рівновага» [36].

Виділені групи принципів вченою є досить дискусійними, адже проставити чітку межу між загальними та специфічними принципами неможливо.

Принципи державного регулювання системи охорони здоров’я містяться в праці Д.М. Рябець:

«- гарантований пакет послуг, що доступний кожному громадянину;

- дотримання національних стандартів якості та професіоналізму;

- взаємоповага пацієнтів та медичних працівників;

- співпраця різних секторів економіки, служб, організацій в інтересах пацієнтів, громад та населення (міжсекторальна взаємодія);

- співвідношення ціна-якість та найбільш ефективне, справедливе та стійке використання обмежених ресурсів;

- багатоукладність економіки охорони здоров'я і багатоначальність її фінансування, поєднання державних гарантій з демонополізацією та заохоченням підприємництва і конкуренції;

- підзвітність громадам і пацієнтам» [64].

Даний підхід є дискусійним з двох точок зору: по-перше, принципи державного регулювання мають відповідати загальним підходам до регулювання в різних сферах суспільного життя, а не лише системи охорони здоров'я; по-друге, зміст зазначених принципів у більшій мірі відповідає вимогам до державного регулювання, аніж принципам, як фундаментальні основи державного управління системою охорони здоров'я.

В контексті другого підходу склад та зміст принципів визначався за різними складовими та механізмами державного управління. Зокрема, вітчизняний вчений В.І. Юнгер присвятив своє дослідження вирішенню проблеми повоєнного відновлення системи охорони здоров'я та запропонував сукупність принципів фінансування повоєнного відновлення, зокрема:

«- прозорість (джерела надходження та напрями витрачання мають бути прозорими, тобто відповідати меті та обліковуватися відповідно до діючого законодавства);

- доброчесність (при формуванні джерел та витрачанні коштів не допускається корупція та порушення законодавства, що стосується обраного порядку акумулювання коштів);

- демократичність (законні джерела надходження коштів не можуть бути обмеженими, а робоча група на демократичних засадах визначає напрями їх витрачання для забезпечення покладених на неї завдань);

- законність (надходження, витрачання, облік та звітування мають відповідати діючому законодавству, що визначатиметься обраним варіантом акумулювання);

- автономність (робоча група самостійно обирає варіант акумулювання, порядок взаємодії із донорами та витрачання коштів для здійснення основної діяльності з розробки Стратегії);

- аполітичність (джерела фінансування діяльності робочої групи не можуть визначати вплив на її роботу та лобіювання конкретних інтересів без їх зазначення в робочих документах, обговореннях та прийняття колективного рішення)» [78].

Криничко Л.Р. вивчала особливості реформування системи охорони здоров'я, та визначила, що ключовим напрямком вирішення системної кризи є управління людськими ресурсами. В даному контексті дослідниця запропонувала власний підхід до управління кадровим потенціалом та запропонувала принципи формування кадрового резерву системи охорони здоров'я.

«- системності - резерв керівних кадрів державного управління системою охорони здоров'я має переглядатися постійно із врахуванням факторів внутрішнього та зовнішнього середовища;

- періодичності - при формуванні резерву керівних кадрів необхідно визначати період, на який він створюється та надавати один із статусів такого резерву: короткостроковий, середньостроковий, довгостроковий;

- плановості - резерв керівних кадрів державного управління системою охорони здоров'я має враховувати стратегічні напрями та плани розвитку системи охорони здоров'я та відповідних органів державного управління;

- гласності - можливість доступу до інформації про результати формування та використання резерву керівних кадрів державного управління системою охорони здоров'я внутрішніх та зовнішніх стейкхолдерів;

- незалежності - уникнення конфлікту інтересів між суб'єктами формування та використання резерву керівних кадрів та претендентів, що можуть бути включенні до резерву;

- рівності - можливість участі у кадровому резерві широкого кола осіб, що відповідають формальним та неформальним характеристикам, які оцінюються» [22].

Принципи державного управління адаптивно-резервною складовою системи охорони здоров'я представлені в дисертаційному дослідженні Курбанова А.К.:

«- системності – державно-управлінські рішення щодо адаптивно-резервного потенціалу повинні формуватися як частина цілісної системи охорони здоров'я, охоплюючи ресурсні, процесні та організаційні аспекти, для досягнення мети системи охорони здоров'я.

- гнучкості – організаційно-методологічні положення державного управління мають бути сформовані таким чином, щоб оперативно змінювати державно-управлінські рішення (кадрового, фінансового, інфраструктурного, медичного характеру), що визначатиме рівень адаптивно-резервного потенціалу системи охорони здоров'я.

- превентивності – державно-управлінські рішення щодо формування адаптивно-резервної складової мають бути спрямовані не лише на реагування, але й на попередження кризових явищ.

- інституційної взаємодії – результативність державного управління адаптивно-резервним потенціалом формується через координацію між суб'єктами державного управління, місцевого самоврядування, міжнародними партнерами, закладами охорони здоров'я, закладами вищої освіти, зацікавленими особами.

- інноваційності – державно-управлінські рішення мають базуватись на впровадженні інноваційних технологій в управління системою охорони здоров'я, процеси реалізації медичних послуг, підготовку медичний кадрів та інші процеси системи охорони здоров'я, що дозволять підвищити рівень адаптивно-резервного потенціалу системи охорони здоров'я.

- обґрунтованості – державно-управлінські рішення мають базуватись на достовірній інформації про розвиток системи охорони здоров'я та прогностичних даних соціально-економічного розвитку та факторів впливу на громадське здоров'я в умовах штаних ситуацій та кризовий явищ.

- контрольованості – процеси, що відбуваються в системі охорони здоров'я та її стратегічному розвитку мають бути контрольовані з боку суб'єктів державного управління для оперативного коригування державноуправлінських рішень щодо підвищення рівня адаптивно-резервного потенціалу та реагування на кризові явища.

- прозорості - забезпечення відкритості, доступності та зрозумілості державно-управлінських рішень, процедур формування і використання резервних ресурсів, а також підзвітності органів влади перед суспільством у процесі реалізації антикризових заходів.

- комплексності - узгоджене поєднання правових, економічних, адміністративних і соціально-комунікаційних інструментів державного впливу з метою забезпечення стійкості, готовності та безперервності медичних послуг у кризових умовах.

- оперативності - здатність органів державної влади та закладів охорони здоров'я своєчасно приймати управлінські рішення, швидко мобілізувати резервні ресурси (перерозподіл фінансових потоків, оперативне залучення медичного персоналу, екстрене розгортання інфраструктурних потужностей) й забезпечувати негайне реагування (функціонування дієвих механізмів антикризової координації) на кризові загрози та надзвичайні ситуації.

- законності - здійснення всіх управлінських дій щодо антикризових заходів та механізмів мобілізації резервних ресурсів виключно в межах чинного законодавства та нормативно-правового регулювання, що передбачає визначеність процедур екстреного фінансування, кадрової мобілізації, використання матеріальних запасів, запровадження надзвичайних режимів функціонування медичних закладів, а також забезпечення дотримання прав пацієнтів і медичних працівників у кризових умовах.

- плановості - визначення стратегічних цілей, пріоритетів, ресурсних потреб і сценаріїв реагування на можливі кризові загрози через забезпечення узгодженості дій органів влади та закладів охорони здоров'я в умовах нестабільності.

- підзвітності – встановлення відповідальності суб'єктів державного управління системою охорони здоров'я за прийняті рішення, використання резервних ресурсів і результати антикризових заходів перед суспільством, державними контролюючими органами та зацікавленими сторонами, що передбачає регулярне звітування за цільовим і ефективним використанням фінансових, кадрових та інфраструктурних резервів.

- компетентності - залучення підготовлених фахівців до планування й реалізації кризового реагування, використання сучасних методів управління ризиками, ефективної координації ресурсів та впровадження доказових управлінських практик у сфері охорони здоров'я.

- справедливості - забезпечення рівного, недискримінаційного та соціально обґрунтованого доступу населення до медичних послуг і резервних ресурсів незалежно від місця проживання, рівня доходів, соціального статусу чи інших характеристик, особливо в умовах кризових ситуацій» [24].

Зважаючи на представлені підходи до формування принципів державного управління системою охорони здоров’я вбачаємо виділити принципи державного управління, які мають відповідати складному об’єкту, а саме: процеси цифрової трансформації системи охорони здоров’я; функціонування цифрової системи охорони здоров’я; процеси розвитку цифрової системи охорони здоров’я. Аналізуючи різні підходи та зважаючи на визначені передумови та фактори цифрової трансформації системи охорони здоров’я, вбачаємо потребу в їх поділі на наступні групи (рис. 2.2):

1. 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. До даних принципів відносимо:

- *принцип стратегічної спрямованості* передбачає узгодження державно-управлінських рішень у сфері цифрової трансформації системи охорони здоров’я з довгостроковими цілями державної політики, прогнозованими потребами населення, напрямами розвитку охорони здоров’я та загальнодержавними пріоритетами цифрового розвитку. Характеризуючи зазначений принцип варто наголосити, що формування та реалізація механізмів цифрової трансформації системи охорони здоров’я має узгоджуватися із стратегічними цілями розвитку системи охорони здоров’я, стратегією економічного розвитку, стратегією повоєнного відновлення України, а отже відповідати етапам реалізації стратегічних документів в цілому та узгоджуватися із діяльністю суб’єктів реалізації державної політики як в сфері охорони здоров’я, так і в інших сферах суспільного розвитку. Це дозволить уникнути сукупності інституційних ризиків, які пов’язані з відсутністю консенсусу між різними гілками влади та суб’єктами державного управління.

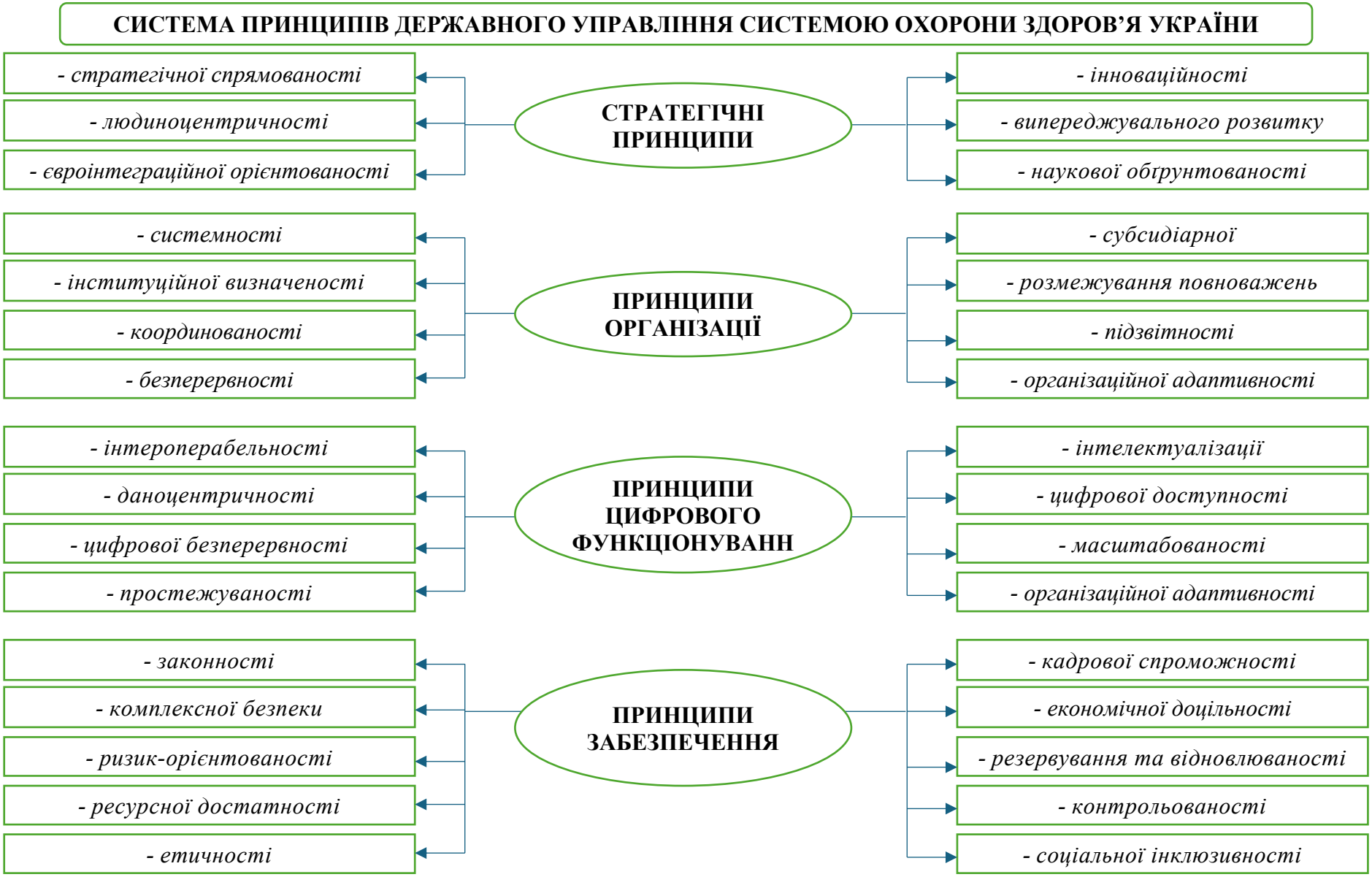


Рис. 2.2. Структура системи принципів державного управління цифровою трансформацією системи охорони здоров'я

- *принцип людиноцентричності* передбачає орієнтацію державного управління цифровим розвитком системи охорони здоров'я на забезпечення прав, законних інтересів, потреб і безпеки людини, визнаючи життя, здоров'я та гідність особи найвищою соціальною цінністю, а цифрові технології - інструментом підвищення якості, своєчасності, безпечності та персоналізації медичної допомоги. Тобто під час розроблення державних цифрових сервісів у сфері охорони здоров'я першочергово враховуються потреби пацієнтів, забезпечується захист їхніх прав, медичної таємниці й персональних даних, а також можливість отримання медичної допомоги відповідно до індивідуальних потреб пацієнта.

- *принцип євроінтеграційної орієнтованості* передбачає формування та реалізацію механізмів державного управління цифровою трансформацією системи охорони здоров’я відповідно до правових, організаційних, інформаційних і технологічних підходів Європейського Союзу та вимог, які висуваються до України відповідно до євроінтеграційних кластерів, що забезпечить інтеграцію національної системи охорони здоров’я в європейський цифровий медичний простір. Це вимагає запровадження технічних і семантичних стандартів, які забезпечують сумісність національних електронних медичних систем із цифровими платформами Європейського Союзу та можливість транскордонного обміну електронними рецептами, медичними записами й іншими даними.

- *принцип інноваційності* передбачає орієнтацію державного управління на створення умов для розроблення, апробації, впровадження та масштабування сучасних цифрових технологій, здатних удосконалювати процеси профілактики, діагностики, лікування, реабілітації, моніторингу стану здоров’я та інформаційної взаємодії між

учасниками системи. Це вимагає створення регуляторних умов для пілотного використання систем штучного інтелекту при оцінці стану громадського здоров’я, діагностування, лікування та реабілітації хворих.

- *принцип випереджувального розвитку* передбачає орієнтацію державно-управлінських рішень не лише на розв’язання поточних проблем цифровізації, а й на прогнозування майбутніх потреб системи охорони здоров’я, технологічних змін, нових ризиків і можливостей із завчасним формуванням необхідного правового, кадрового, інформаційного та інфраструктурного забезпечення. Досить важливим є реалізація даного принципу в контексті прогнозування майбутнього зростання обсягів медичних даних і використання штучного інтелекту з одночасним розвитком центрів обробки даних, підготовкою фахівців, удосконаленням законодавства та встановленням вимог до безпечності алгоритмічних рішень.

- *принцип наукової обґрунтованості* передбачає, що формування та реалізація механізмів державного управління цифровою трансформацією системи охорони здоров’я повинні ґрунтуватися на результатах наукових досліджень, доказовій медицині, об’єктивних даних, прогнозуванні, міжнародному досвіді та оцінці ефективності цифрових технологій, забезпечуючи прийняття обґрунтованих, ефективних і перспективних державно-управлінських рішень. Розроблення державної стратегії цифрового розвитку системи охорони здоров'я має відбуватися на основі результатів наукових досліджень, аналізу медичних даних, міжнародних практик і прогнозування майбутніх потреб системи. Так наприклад, прийняття рішення про впровадження систем штучного інтелекту в медичній практиці лише після проведення клінічної валідації, оцінювання їх безпечності, ефективності, економічної доцільності та відповідності міжнародним стандартам.

2. Принципи організації – є 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. До даних принципів пропонуємо відносити:

- *принцип системності* забезпечує урахування взаємозв'язків між усіма складовими системи охорони здоров'я, охоплюючи клінічні, організаційні, кадрові, інформаційні, технологічні, правові та ресурсні процеси при формуванні механізмів державного управління цифровою трансформацією. Відповідно до зазначеного принципу цифрова трансформація має передбачати не лише впровадження технологічного рішення, але й одночасну підготовку персоналу, розроблення нормативних вимог, забезпечення технічної інфраструктури та організацію обміну даними між закладами охорони здоров'я.

- *принцип інституційної визначеності* передбачає чітке встановлення складу суб'єктів державного управління цифровою трансформацією системи охорони здоров'я, їхніх функцій, повноважень, сфер відповідальності та меж втручання. Тобто, є потреба у нормативному розмежуванні повноважень між центральними органами виконавчої влади, органами місцевого самоврядування, власниками електронної системи охорони здоров'я та закладами охорони здоров'я щодо впровадження, використання і захисту цифрових сервісів.

- *принцип інституційної взаємодії* визначає узгоджену співпрацю органів державної влади, органів місцевого самоврядування, закладів охорони здоров'я, наукових установ, розробників цифрових технологій, міжнародних партнерів та інших заінтересованих суб'єктів. Реалізація зазначеного

принципу можлива через формування міжвідомчої координаційної ради, до складу якої входять представники органів влади, медичних закладів, наукового середовища, ІТ-сектору та громадських організацій.

- *принцип координованості* означає узгодження цілей, рішень, строків і дій суб'єктів державного управління на державному, регіональному, місцевому та інституційному рівнях для недопущення дублювання функцій і фрагментарності цифрових проєктів. Реалізація зазначеного принципу передбачає погодження регіональних програм цифровізації охорони здоров'я із загальнодержавною стратегією, технічними стандартами та календарним планом упровадження національних цифрових сервісів.

- *принцип субсидіарності передбачає* прийняття державно-управлінських рішень на тому рівні, на якому вони можуть бути реалізовані найбільш результативно, із переданням на вищий рівень лише тих повноважень, які потребують централізованого регулювання, стандартизації або координації. Відповідно держава встановлює єдині стандарти даних і кібербезпеки, тоді як органи місцевого самоврядування та заклади охорони здоров'я самостійно визначають порядок організації навчання персоналу й упровадження локальних цифрових сервісів, що дозволить досягти високого рівня децентралізації влади та автономії управління суб'єктами реалізації медичних послуг.

- *принцип розмежування повноважень і відповідальності* передбачає закріплення за кожним суб'єктом конкретних завдань, прав, обов'язків і відповідальності за прийняті рішення, використані ресурси та результати цифрової трансформації системи охорони здоров'я. Це вимагає визначення відповідальних суб'єктів за якість медичних даних, технічну працездатність інформаційної системи, захист інформації, навчання користувачів і реагування на цифрові інциденти.

- *принцип підзвітності* передбачає обов'язок суб'єктів державного управління звітувати про прийняті рішення, використання фінансових та інших ресурсів, виконання цифрових проєктів і досягнуті результати перед державою, суспільством та іншими заінтересованими сторонами. Напрямом реалізації зазначеного принципу може бути оприлюднення регулярних звітів про виконання державних програм цифровізації, використання бюджетних коштів, кількість підключених закладів і досягнуті показники доступності цифрових медичних послуг.

- *принцип компетентності* передбачає залучення до формування та реалізації державно-управлінських рішень фахівців, які мають необхідні професійні, управлінські, медичні, правові та цифрові компетентності. Відповідно є потреба включення до робочих груп медичних працівників, фахівців із публічного управління, інформаційних технологій, кібербезпеки, захисту персональних даних і медичного права.

- *принцип безперервності управлінського циклу* передбачає послідовне здійснення планування, організації, реалізації, моніторингу, оцінювання та коригування державно-управлінських рішень упродовж усього життєвого циклу цифрових технологій. Так, після впровадження електронного сервісу держава організовує постійний моніторинг його роботи, оцінювання результативності, збір відгуків користувачів та періодичне оновлення функціоналу.

- *принцип організаційної адаптивності* передбачає здатність суб'єктів державного управління своєчасно змінювати структури, процедури, форми взаємодії та розподіл функцій відповідно до технологічних змін, нових потреб системи охорони здоров'я та впливу зовнішніх чинників. Вимагає оперативного формування спеціалізованих координаційних підрозділів або зміни порядку інформаційної взаємодії у разі впровадження нових систем штучного інтелекту, платформ обміну даними чи телемедичних сервісів.

3. 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 цифрового функціонування формуються на основі властивостей цифрової системи охорони здоров'я і визначають правила їх забезпечення в процесі державного управління. Складовими даних принципів є:

- *принцип інтероперабельності* передбачає забезпечення організаційної, технічної, семантичної та правової сумісності цифрових інформаційних систем, що забезпечує безперервний обмін медичними даними та інформаційну взаємодію між усіма суб'єктами системи охорони здоров'я. Так, цифрова система охорони здоров’я забезпечує автоматичний обмін медичною інформацією між сімейним лікарем, спеціалізованими медичними закладами, лабораторіями та аптечними закладами без повторного внесення даних.

- *принцип даноцентричності* передбачає використання якісних, достовірних, актуальних і структурованих даних як основи для формування, реалізації, моніторингу та оцінювання державно-управлінських рішень, а також прийняття клінічних рішень. Це вимагає використання єдиного електронного медичного запису пацієнта як основного джерела інформації для надання медичної допомоги, аналітики та прогнозування розвитку системи охорони здоров’я.

- *принцип цифрової безперервності* передбачає забезпечення постійної доступності цифрових сервісів, інформаційних систем та електронних медичних ресурсів незалежно від часу, місця, технічних або організаційних умов їх використання. Відповідно є потреба в забезпеченні безперервного функціонування електронної системи охорони здоров’я, резервного копіювання даних і можливості отримання електронних медичних послуг у режимі 24/7.

- *принцип простежуваності* передбачає можливість ідентифікації, документування та відстеження всіх операцій із медичними даними, цифровими сервісами та державно-управлінськими рішеннями протягом усього життєвого циклу їх реалізації. Тобто, автоматична реєстрація всіх дій користувачів в електронній системі охорони здоров'я із фіксацією часу, змісту змін та особи, яка їх здійснила.

- *принцип інтелектуалізації* передбачає використання технологій штучного інтелекту, аналітики великих даних, прогнозних моделей та систем підтримки прийняття рішень для підвищення обґрунтованості управлінських і клінічних рішень. Як приклад, застосування алгоритмів штучного інтелекту для прогнозування поширення захворювань, підтримки клінічної діагностики та аналізу ефективності державної політики у сфері охорони здоров’я.

- *принцип цифрової доступності* передбачає забезпечення безперервного, надійного та технічно можливого доступу авторизованих користувачів до цифрових сервісів, інформаційних систем, медичних даних і цифрової інфраструктури незалежно від місця підключення, часу використання, програмно-технічної платформи чи використовуваного пристрою. Це вимагає забезпечення функціонування електронної системи охорони здоров'я через веб-інтерфейс, мобільний застосунок та інтегровані медичні інформаційні системи із підтримкою різних операційних систем, типів пристроїв і захищених каналів зв'язку без втрати функціональних можливостей.

- *принцип масштабованості* передбачає можливість розширення функціональних можливостей цифрової системи охорони здоров’я, збільшення кількості користувачів, цифрових сервісів та обсягів медичних даних без втрати ефективності її функціонування. Реалізація зазначеного можлива через поетапне підключення нових медичних закладів, цифрових сервісів і модулів до єдиної електронної системи охорони здоров'я без необхідності зміни її базової архітектури.

- *принцип технологічної адаптивності* передбачає здатність цифрової архітектури системи охорони здоров'я забезпечувати інтеграцію нових технологічних компонентів, модернізацію програмно-технічних рішень, зміну архітектури інформаційних систем та розширення їх функціональних можливостей без порушення цілісності, сумісності, безперервності функціонування та інформаційної взаємодії цифрової системи. Зокрема, модернізація електронної системи охорони здоров'я шляхом інтеграції нового модуля штучного інтелекту або телемедичної платформи без необхідності зміни базової архітектури системи, припинення її роботи чи повторного проєктування інших інформаційних компонентів.

4. 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.

- *принцип законності* передбачає формування, реалізацію та розвиток цифрової системи охорони здоров’я виключно відповідно до норм міжнародного і національного законодавства, з дотриманням прав і свобод людини, вимог щодо захисту персональних даних, медичної таємниці, електронної взаємодії та застосування систем штучного інтелекту. Відповідно є потреба впровадження цифрового сервісу для оброблення медичних даних лише після визначення законних підстав їх збору, доступу, використання, передачі та зберігання.

- *принцип комплексної безпеки* передбачає одночасне забезпечення інформаційної, кібернетичної, технологічної та медичної безпеки цифрової системи охорони здоров’я з метою захисту пацієнтів, медичних працівників, медичних даних, цифрових сервісів та об’єктів інфраструктури. Це вимагає проведення комплексного оцінювання безпеки

інформаційної системи, яке охоплює захист даних, контроль доступу, стійкість до кібератак, надійність програмного забезпечення та можливий вплив його помилок на безпечність медичної допомоги.

- *принцип ризик-орієнтованості* передбачає систематичне виявлення, оцінювання, попередження та мінімізацію правових, інформаційних, кібернетичних, технологічних, організаційних, кадрових і соціальних ризиків на всіх етапах цифрового розвитку системи охорони здоров'я. Перед впровадженням системи штучного інтелекту здійснюється оцінювання ризиків помилкових рекомендацій, дискримінаційних алгоритмів, витоку даних, технічних відмов та надмірної залежності медичного працівника від автоматизованого рішення.

- *принцип ресурсної достатності* передбачає забезпечення цифрового розвитку системи охорони здоров'я необхідними фінансовими, кадровими, технічними, технологічними, інформаційними та інфраструктурними ресурсами відповідно до визначених цілей, масштабів і складності цифрових рішень. Прикладом реалізації даного принципу є впровадження нового електронного медичного сервісу, що супроводжується фінансуванням закупівлі обладнання, оновленням мереж, підготовкою персоналу, технічною підтримкою та подальшим обслуговуванням системи.

- *принцип кадрової спроможності* передбачає забезпечення належного рівня професійних і цифрових компетентностей медичних працівників, управлінського персоналу, фахівців з інформаційних технологій та інших осіб, залучених до формування, використання і розвитку цифрової системи охорони здоров'я. Так, є потреба в організації безперервного навчання медичних працівників щодо роботи з електронними медичними записами, телемедичними сервісами, засобами захисту інформації та системами підтримки клінічних рішень.

- *принцип економічної доцільності* передбачає прийняття державно-управлінських рішень щодо впровадження і розвитку цифрових технологій на основі співвідношення необхідних витрат та очікуваних медичних, соціальних, управлінських і економічних результатів. Так, перед масштабуванням цифрової платформи оцінюються витрати на її створення, експлуатацію та оновлення, а також очікуване скорочення адміністративних витрат, часу обслуговування пацієнтів і дублювання медичних досліджень.

- *принцип резервування та відновлюваності* передбачає створення резервних технічних потужностей, каналів зв'язку, копій даних і процедур аварійного відновлення, необхідних для своєчасного поновлення функціонування цифрової системи охорони здоров'я після технічних збоїв, кібератак або надзвичайних ситуацій. Саме тому має здійснюватися регулярне резервне копіювання електронних медичних даних із їх зберіганням у відокремлених захищених середовищах та періодична перевірка процедур відновлення інформаційних систем.

- *принцип контрольованості* передбачає постійний моніторинг функціонування цифрової системи охорони здоров'я, оцінювання результативності цифрових рішень, контроль використання ресурсів і встановлення відповідальності суб'єктів за прийняті рішення, виконані дії та отримані результати. Прикладом реалізації є формування системи показників цифрового розвитку, регулярне проведення аудиту цифрових проєктів та оприлюднення звітів про використання бюджетних коштів, працездатність сервісів і досягнуті результати.

- *принцип етичності* передбачає використання цифрових технологій і систем штучного інтелекту з дотриманням людської гідності, автономії пацієнта, недискримінації, справедливості, конфіденційності та пріоритету інтересів людини над технологічною доцільністю. Застосування системи штучного інтелекту для підтримки клінічних рішень за умови

інформування пацієнта має здійснюватися із збереженням контролю медичного працівника та перевірки алгоритму на наявність дискримінаційних результатів.

- *принцип соціальної інклюзивності* передбачає спрямування державної політики цифрового розвитку системи охорони здоров'я на недопущення цифрового та соціального виключення окремих категорій населення, забезпечення рівних можливостей отримання медичної допомоги та врахування потреб осіб, які через вік, стан здоров'я, інвалідність, низький рівень доходів, місце проживання, недостатню цифрову грамотність або інші соціальні обставини мають обмежені можливості використання цифрових медичних сервісів. Це вимагає запровадження державних програм розвитку цифрової грамотності населення, організації допомоги соціальних і медичних працівників під час користування електронними сервісами, забезпечення громадських пунктів доступу до них, а також збереження альтернативних каналів запису на прийом, отримання медичної інформації та взаємодії із закладами охорони здоров'я для соціально вразливих груп населення.

Таким чином, 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 до їх змісту. Для вирішення зазначеного розроблено багаторівневу структуру державного управління цифровою трансформацією та цифровою системою охорони здоров'я, зокрема: до стратегічних принципів (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) відносяться стратегічної спрямованості, людиноцентричності, євроінтеграційної орієнтованості, інноваційності, випереджувального розвитку, наукової обґрунтованості; до 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) відносяться системності, інституційної визначеності, інституційної взаємодії, координованості, субсидіарності, розмежування повноважень і відповідальності, підзвітності, компетентності, безперервності управлінського циклу, організаційної адаптивності; до принципів 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) відносяться інтероперабельності, даноцентричності, цифрової безперервності, простежуваності, інтелектуалізації, цифрової доступності, масштабованості, технологічної адаптивності; до принципів забезпечення (сукупність фундаментальних положень, які визначають правові, фінансово-економічні, кадрові, інформаційні та безпекові умови формування, функціонування і подальшого розвитку цифрової системи охорони здоров'я) відносяться законності, комплексної безпеки, ризик-орієнтованості, ресурсної достатності, кадрової спроможності, економічної доцільності, резервування та відновлюваності, контрольованості, етичності, соціальної інклюзивності.

2.3. Методологічні положення державного управління цифровою трансформацією системи охорони здоров'я

Цифрова трансформація системи охорони здоров'я як об'єкт державного управління має сукупність властивостей, які впливають на теоретико-методологічні положення прийняття та реалізації державно-управлінських рішень. «На даному етапі розвитку нашої країні та в умовах фінансової, політичної, соціальної кризи держава не має можливості чітко та стабільно забезпечити якісне медичне обслуговування громадян, однак забезпечення права людини на кваліфіковані, якісні, професійні та доступні медичну допомогу та послуги, що передбачені законодавством України та міжнародними стандартами, є найважливішим орієнтиром. Оскільки сфера охорони здоров'я стосується абсолютно кожного громадянина України, то Міністерство охорони здоров'я має бути одним із лідерів діджиталізації в країні. Приклад вдалої трансформації в цьому напрямку стає можливим при об'єднанні процесу діджиталізації та реформування медичної системи через продовження впровадження нових моделей функціонування та фінансування у відповідності до чинних норм та стандартів Європейського Союзу» [77].

Зокрема, це впливає на методологічні положення в частині об'єктно-предметногов частині поля державного управління, мети, завдань, механізмів. Адже відбувається модифікація не лише об'єкту державного управління, а саме процесів цифрової трансформації, але й трансформація самої системи охорони здоров'я та її функціонування в інших просторових та часових вимірах.

«Справжня цінність цифрових рішень у соціальному секторі визначається не лише технологіями, а й здатністю держави забезпечити справедливість, доступність і довіру в новому цифровому контексті. Лише за такої умови цифрова трансформація стане не самоціллю, а інструментом

побудови соціальної держави нового покоління – гнучкої, інклюзивної та орієнтованої на людину» [66].

В той же час цифрова трансформація призводить до змін у функціонуванні суб'єктів державного управління та власне методологічній дії впливу суб'єкту на об'єкт. Методологічна дія обумовлює потребу в удосконаленні економічних, правових, організаційних та інформаційних механізмів державно-управлінського впливу. Все обумовлює потребу в удосконаленні методологічних положень державного управління, що має забезпечити структурування та визначення векторів розвитку методологічних положень.

Зазначені питання частково визначені в працях вітчизняних вчених: 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.

«Сфера електронної системи охорони здоров'я тільки робить перші кроки в напрямку цифрового перетворення. Деякі країни обганяють інші, але не можливо назвати це явище глобальним. Завдяки доступній технології цифрового охорони здоров'я, яка постійно вдосконалюється і модернізується, стає можливим побачити новий більш ефективний і майже бездоганний образ охорони здоров'я в Україні» [18].

Відповідно державна політика щодо цифрової трансформації системи охорони здоров'я має враховувати сукупність положень зокрема:

- євроінтеграційні процеси є пріоритетними для держави, а тому усі процеси цифрової трансформації мають відбуватися не всупереч, а в

контексті євроінтеграції, щоб забезпечити інтеграцію національної системи охорони здоров’я України в європейський медичний простір;

- цифрова трансформація національної системи охорони здоров’я має забезпечити, щоб впроваджене програмне забезпечення, інформаційні системи і технології були сумісні з цифровими платформами Європейського Союзу в цілому та країн-членів Європейського Союзу;

- процеси цифрової трансформації мають відбуватися у відповідності до норм міжнародного та національного законодавства таким чином, щоб не порушувати гарантовані права та свободи людини та громадянина, захисту персональних даних, медичної таємниці та етичних засад використання цифрових технологій і систем штучного інтелекту;

- цифрова система охорони здоров’я має функціонувати в контексті забезпечення принципів безпеки держави, регіонів та окремих суб’єктів;

- впровадження інноваційних технологій мають орієнтуватися на прогресивні технології майбутнього та бути адаптивними до змін, що будуть відбуватися в ІТ-сфері в контексті розвитку наукових досліджень;

- впровадження цифрових технологій має супроводжуватися системною ідентифікацією, оцінюванням та управлінням технологічними, інформаційними, кібернетичними, правовими й організаційними ризиками;

- цифрова трансформація повинна супроводжуватися безперервним розвитком цифрових компетентностей медичних працівників, управлінського персоналу та населення, забезпечуючи ефективне використання цифрових сервісів;

- рішення щодо цифрової трансформації повинні ґрунтуватися на результатах наукових досліджень, доказовій медицині, міжнародних стандартах і найкращих практиках застосування цифрових технологій у сфері охорони здоров'я;

- процеси цифрової трансформації системи охорони здоров'я мають здійснюватися на основі чітко визначеного розподілу повноважень,

відповідальності та координації діяльності між усіма суб'єктами їх реалізації, зокрема органами державної влади, органами місцевого самоврядування, закладами охорони здоров'я, розробниками цифрових технологій, науковими установами, міжнародними партнерами та інститутами громадянського суспільства;

- цифрова трансформація системи охорони здоров'я має супроводжуватися розвитком організаційної, кадрової та технічної спроможності суб'єктів її реалізації, необхідної для ефективного впровадження, супроводу та розвитку цифрових технологій;

- процеси цифрової трансформації повинні базуватися на використанні якісних, достовірних, актуальних і захищених медичних даних як основи для прийняття клінічних та управлінських рішень;

- рішення щодо цифрової трансформації системи охорони здоров'я повинні прийматися на основі оцінки їх економічної доцільності, очікуваної ефективності, довгострокової стійкості та впливу на якість і доступність медичної допомоги;

- державна політика цифрової трансформації системи охорони здоров'я має бути спрямована на формування довіри населення до цифрових медичних сервісів, підвищення рівня цифрової грамотності, забезпечення відкритості цифрових рішень та стимулювання їх широкого використання;

- процеси цифрової трансформації системи охорони здоров'я повинні здійснюватися за умови наявності послідовної політичної підтримки, що забезпечує стратегічну наступність державної політики, нормативно-правове забезпечення, належне фінансування та координацію діяльності суб'єктів її реалізації.

Зазначене визначає специфіку методологічних положень державного управління системою охорони здоров’я, адже реформуванню підлягає як

власне система охорони здоров’я як об’єкт державного управління, так і діяльність суб’єктів державного управління та процес прийняття державно-управлінських рішень. «Державне управління є одним з основних видів управління в суспільстві - соціального управління, що насамперед обумовлено особливістю правового статусу його головного суб’єкта - держави, яка свій владний вплив поширює на все суспільство і навіть поза його межі. Зважаючи на те, що в державному управлінні задіяні десятки мільйонів людей, величезна кількість державних органів і посадових осіб, воно потребує різноманітних ресурсів: матеріальних, фінансових, інтелектуальних, інформаційних тощо. Держава, реалізуючи правотворчу функцію, встановлює загальні правила (вимоги, норми) поведінки людей у всіх сферах суспільного життя, а також забезпечує їх дотримання можливістю застосування державного примусу. Проте, примусовість - не головний, а допоміжний фактор упорядкованості суспільних відносин. Головним пріоритетом діяльності будь-якої демократичної держави повинно стати забезпечення реалізації прав, свобод і законних інтересів її населення, служіння йому» [37].

Складовими методологічних положень державного управління цифровою трансформацією системи охорони здоров’я є наступні: об’єктно-предметне поле державного управління; мета та завдання державного управління цифровізацією системи охорони здоров’я та методи здійснення управлінського впливу, що реалізується через механізми державного управління. Розглянемо детально кожну із вказаних складових.

Питання змісту об’єкту та предмету державного управління цифровою трансформацією системи охорони здоров’я є складним питанням, що обумовлено сукупністю причин:

- по-перше, багатосуб'єктність державного управління та процесів цифрової трансформації. Так, до процесів цифрової трансформації системи охорони здоров'я залучені суб'єкти, які знаходяться в системі реалізації медичних послуг, а саме: розробники цифрових технологій, суб'єкти обслуговування цифрових технологій, суб'єкти цифрової інфраструктури, суб'єкти забезпечення кібербезпеки та інші. В той же час, суб'єктна структура державного управління також є досить широкою, адже залучені суб'єкти державного управління, які реалізують не лише політику в сфері охорони здоров'я, але й суб'єкти, які реалізують інформаційну політику, політику цифрової трансформації, економічну та євроінтеграційну політику та інші. Крім того, до процесів цифрової трансформації мають бути залучені міжнародні партнери як в якості донорів, так і в якості експертів, а також інститути громадянського суспільства для врахування суспільних інтересів.

- по-друге, комплексний характер, адже цифрова трансформація стосується як медичної складової, так і фінансової, управлінської, інформаційної, комунікаційної, кадрової та організаційної. Так, медичні послуги піддаються найбільшим змінам в умовах цифрової трансформації, як з позиції діагностування, лікування, реабілітації та профілактики із застосуванням комп'ютерних технологій та технологій штучного інтелекту, так і з позиції повністю цифрової медичної послуги на основі положень телемедицини. В той же час цифрові технології впливають на управлінські процеси в частині взаємодії між суб'єктами державного управління та між суб'єктами та об'єктами управління, що вимагає змін в інформаційно-комунікаційній системі, організації такої взаємодії та підготовки і перепідготовки професійних кадрів, які володіють цифровими технологіями.

- по-третє, багаторівневість системи управління, адже управлінські рішення формуються і реалізуються на міжнародному (відповідність вимогам ВООЗ та ЄС), державному, регіональному, місцевому та інституційному рівнях, що потребує узгодження цілей, повноважень і ресурсів.

- по-четверте, комплексність управлінського впливу. Так, цифрова трансформація передбачає одночасне застосування правових, організаційних, економічних, кадрових, інформаційних, технологічних та безпекових механізмів державного управління, які повинні функціонувати узгоджено для досягнення єдиної стратегічної мети.

- по-п’яте, динамічність об’єкта державного управління. Цифрова трансформація характеризується постійним розвитком цифрових технологій, зміною нормативно-правового середовища, появою нових цифрових ризиків, трансформацією моделей надання медичних послуг та еволюцією потреб населення, що обумовлює необхідність безперервного оновлення управлінських рішень та механізмів їх реалізації.

Відповідно об’єкт державного управління є складним, динамічним та таким, що охоплює різні сфери суспільних відносин, що знаходяться поза системою охорони здоров’я, адже цифрова трансформація системи охорони здоров’я - це не просто впровадження окремих технологій, а глибока перебудова того, як збираються, зберігаються, передаються й використовуються медичні дані, як пацієнт взаємодіє з системою і як приймаються клінічні та управлінські рішення.

З цього випливає, що об’єктом державно-управлінського впливу виступатимуть:

1. Процеси цифрової трансформації системи охорони здоров’я, що є складною сукупністю відносин, які передбачають: 1) оцифрування медичної інформації, тобто перехід від паперових документів до даних

(паперова документація замінюється структурованими цифровими даними, які можна швидко знайти, оновити й передати між закладами (електронні направлення, електронні рецепти, декларації з лікарями первинної ланки, електронна історія хвороби та інше); 2) розробка та впровадження єдиних стандартів обміну даними для забезпечення руху інформації між рівнями медичної допомоги, закладами охорони здоров'я та суб'єктами державного управління); 3) впровадження інструментів дистанційної медицини шляхом запровадження онлайн-консультацій, дистанційного моніторингу хронічних хворих, телерадіології, консиліумів між лікарями різних закладів; 4) запровадження технологій аналітики даних для підтримки клінічних рішень, а також управління усіма видами діяльності закладів охорони здоров'я та системою охорони здоров'я загалом; 5) запровадження технологій штучного інтелекту в процеси діагностики, лікування, прогнозування та попередження захворювань; 5) інфраструктурна модернізація, що передбачає перехід на хмарні рішення, побудову центрів обробки даних, розвиток мобільного зв'язку та широкосмугового доступу, для забезпечення масштабування цифрової трансформації; 6) запровадження інструментів кібербезпеки та захисту даних, адже при цифровізації обов'язковим процесом є побудова систем шифрування, розмежування доступу, приведення у відповідність нормам захисту персональних даних; 7) формування, розподіл та використання фінансових ресурсів для забезпечення процесів цифрової трансформації, адже даний етап є найбільш ресурсномістким. Державне управління зазначеними процесами має бути системним, тобто при зміні одного процесу забезпечити коригування або ж зміну інших.

Процеси цифрової трансформації досить активно сьогодні відбуваються в Україні, про що свідчать значні трансформаційні зміни у 2025 році:

«- реформа МСЕК і цифрова система оцінювання повсякденного функціонування. Запрацювала реформована цифрова система оцінювання повсякденного функціонування людини. ІТ-рішення отримало GovTech Award 2025 як одна з найкращих держтех-реформ року. Уже опрацьовано понад 500 тисяч справ, уся статистика доступна в реальному часі;

- електронний рейтинговий розподіл в інтернатуру. Уперше в історії медичної освіти розподіл студентів в інтернатуру відбувся в електронному форматі. Система гарантує рівний доступ і унеможливлює будь-яке втручання в процес. Понад 2,5 тисячі лікарів-інтернів розпочали інтернатуру після цифрового розподілу;

- нові державні реєстри та цифрові системи. У 2025 році ДП «Електронне здоров'я» розробило та адмініструє: електронну чергу на безоплатне ендопротезування; систему електронної нотифікації косметичної продукції; державний реєстр дезінфекційних засобів. Також розроблено: ліцензійний реєстр суб'єктів системи крові; цифрові ліцензії щодо обігу наркотичних засобів, психотропних речовин і прекурсорів (бета-тестування);

- телемедицина та міжнародна співпраця. Запущено україно-французький телемедичний проєкт для дистанційної діагностики пацієнтів. До українських медзакладів доставлено 142 одиниці телемедичного обладнання на суму понад 4 млн євро;

- розвиток ЕСОЗ і нові цифрові сервіси. Протягом року в електронній системі охорони здоров'я реалізовано низку важливих змін: нові інтеграції з державними реєстрами та альтернативні канали сповіщення пацієнтів (Дія, Viber); міжнародні інструменти оцінювання стану пацієнтів; відпуск налбуфіну та буторфанолу за е-рецептом; призначення та відпуск ДЗР за е-запитом; облік медичного обладнання. Уперше запущено Особистий

кабінет пацієнта - інструмент доступу до персональних даних і декларацій в ЕСОЗ;

- транскордонний обмін даними. Отримано грант на реалізацію спільного проєкту України та Естонії з підключення до мережі MyHealth@EU - частини Європейського простору даних охорони здоров'я» [74].

2. Функціонування системи охорони здоров'я під час цифрової трансформації. Функціонування системи охорони здоров'я під час цифрової трансформації складає собою сукупність взаємопов'язаних медичних, управлінських, інформаційних, організаційних, ресурсних, аналітичних та безпекових процесів, що забезпечують безперервне функціонування системи охорони здоров'я в умовах впровадження цифрових технологій, інформаційної взаємодії, автоматизації діяльності та використання цифрових даних для надання медичних послуг і реалізації державної політики.

Ключова особливість цього періоду в тому, що система працює у двох режимах одночасно. Частина процесів уже переведена в цифру, частина ще залишається паперовою чи ручною, і система мусить забезпечувати їхню сумісність. Наприклад, в Україні лікар первинної ланки вже працює з електронною карткою пацієнта й е-рецептом, але вузький спеціаліст у тому ж регіоні може ще вести записи частково на папері. Тому функціонування в перехідний період характеризується гібридністю - паралельним існуванням старих і нових практик.

В перехідний період виникає характерний виклик, що характеризується нерівномірністю якості та повноти даних, адже частина історії хвороби залишилася на папері й у цифрове середовище не потрапила. Тому система функціонує з прогалинами, які поступово заповнюються. Така ситуація також загострюється відсутністю інтероперабельності, через несумісність різних інформаційних систем та реєстрів, що також може сприяти її вразливості до кіберзагроз та порушення приватності медичних даних. Дані загрози

обумовлені паралельним існуванням двох систем та внесенням неправдивих або спотворених даних до цифрової системи. Важливим інструментом вирішення зазначених проблем нецифрового характеру є здійснення заходів з адаптації пацієнтів, лікарів, медичного, обслуговуючого та управлінського персоналу, через здобуття ними відповідних навичок та забезпечення різного доступу до цифрових систем.

Державне управління системою охорони здоров'я на даному етапі характеризується прийняттям державно-управлінських рішень для стабілізації стану системи та забезпечення керованості процесів переведення системи з однієї системи в іншу.

3. Функціонування цифрової системи охорони здоров'я. Повністю цифрова система охорони здоров'я характеризується управлінськими, організаційними, медичними та забезпечувальними процесами, що відбуваються в цифровому середовищі. У повністю цифровій системі охорони здоров'я кожен пацієнт має єдиний наскрізний електронний медичний запис, який існує не в конкретному закладі, а в централізованій цифровій інфраструктурі. Усе, що відбувається з пацієнтом, записується в цей єдиний профіль у стандартизованому форматі, а заклад чи лікар не володіє даними, а лише отримує до них доступ за обмеженими правами, щодо зміни даних або їх розширення. На основі таких даних приймаються державно-управлінські рішення та здійснюється фінансування системи охорони здоров'я. Зріла цифрова система функціонує як багатошарова архітектура: 1) інфраструктура (хмара, мережі, пристрої); 2) дані (наприклад, єдиний медичний запис у стандартному форматі); 3) шар обміну й інтероперабельності, що з'єднує всіх учасників; 4) прикладний шар (застосунки для лікарів, пацієнтів, аптек, управлінців та алгоритми ШІ); 5) шар безпеки й управління доступом, що пронизує всі рівні. Кожен учасник працює зі своїм інтерфейсом, але всі спираються на один спільний масив даних. Цифрова система охорони здоров'я функціонує як єдиний

інформаційний організм, де дані пацієнта безперервно й безпечно циркулюють між усіма учасниками, рішення підкріплені аналітикою й штучним інтелектом, допомога надається проактивно й часто дистанційно, а сам пацієнт стає центром і активним учасником процесу, а жодна ланка не працює ізольовано.

Таким чином, виходячи з визначених трьох блоків, об’єкт державного управління цифровою трансформацією системи охорони здоров’я структурно включає:

- процеси трансформації: оцифрування медичної інформації, забезпечення інтероперабельності, розвиток телемедицини, впровадження аналітики та штучного інтелекту, розбудову пацієнтоцентричних сервісів, модернізацію інфраструктури, кібербезпеку й управлінську цифровізацію;

- ресурси та інфраструктуру: електронну систему охорони здоров'я та її центральні компоненти, дані (єдиний медичний запис), хмарні потужності, мережі, медичне обладнання, програмне забезпечення;

- учасників відносин: заклади охорони здоров’я, фармацевтичні компанії, медичний, обслуговуючий та управлінський персонал, пацієнтів, страхові компанії, ІТ-компанії, органи державного управління та суб’єкти місцевого самоврядування.

- медичні та суміжні послуги: реалізуються в гібридному режимі (співіснування паперової та цифрової форми) в процесі цифрової трансформації та повністю цифровому середовищі при цифровій системі охорони здоров’я.

- управлінські процеси: між суб’єктами державного управління та місцевого самоврядування; між суб’єктами державного управління, місцевого самоврядування та закладами охорони здоров’я / пацієнтами / ІТ-компаніями; між закладами охорони здоров’я та пацієнтами; між закладами охорони здоров’я та ІТ-компаніями.

Відповідно державне управління здійснюється не статичним станом, а керованим переходом як під час цифрової трансформації, так і при повністю цифровізованій системі охорони здоров’я, яка теж є динамічною, адже має постійно удосконалюватися під впливом як медичних інновацій, так і техніко-технологічних.

Виходячи із зазначеного можемо сформулювати зміст об’єктно-предметного поля державного управління цифровою трансформацією системи охорони здоров’я:

- *об'єкт державного управління цифровою трансформацією системи охорони здоров'я* - це сукупність суспільних відносин, процесів, ресурсів та інституцій сфери охорони здоров’я, на які здійснюється державно-управлінський вплив органів державного управління та місцевого самоврядування з метою керованого переведення системи охорони здоров’я у цифровий режим функціонування із забезпеченням сумісності, безпеки та доступності медичних даних для підвищення якості, ефективності, прозорості та результативності медичної допомоги.

- *предмет державного управління цифровою трансформацією системи охорони здоров’я* – це управлінський вплив на суспільні відносини, процеси, ресурси та інституції сфери охорони здоров’я для забезпечення керованого переведення системи охорони здоров’я у цифровий режим функціонування із забезпеченням сумісності, безпеки та доступності медичних даних для підвищення якості, ефективності, прозорості та результативності медичної допомоги, що здійснюється суб’єктами державного управління та місцевого самоврядування шляхом застосування сукупності механізмів.

Мета державного управління цифровою трансформацією системи охорони здоров’я – це формування та реалізація правових, організаційних, інформаційних, фінансових та кадрових механізмів державно-

управлінського впливу для забезпечення керованого переходу системи охорони здоров'я до цілісної, безпечної та інтероперабельної цифрової екосистеми охорони здоров’я, у якій медичні дані безперервно, захищено й доступно циркулюють між усіма учасниками для підвищення доступності, якості, безпеки, ефективності й людиноцентричності охорони здоров'я.

Відповідно до визначеного змісту об’єкту, предмету та мети державного управління цифровою трансформацією системи охорони здоров’я, можемо визначити наступну сукупність ключових завдань:

- оновлення та розробка нормативно-правового забезпечення процесів цифрової трансформації системи охорони здоров’я, що забезпечить процес інтеграції національної системи охорони здоров’я в європейський медичний простір;

- створення багаторівневої системи кіберзахисту національних реєстрів, забезпечення резервування даних, протидії кібератакам та збереження конфіденційності медичної інформації пацієнтів;

- розробити та впровадити нормативно-правові акти щодо телемедицини, які регулюють порядок надання онлайн-консультацій, здійснення віддаленого моніторингу та телерадіології;

- оновлення кримінального законодавства в частині встановлення кримінальної відповідальності за кіберзлочини в сфері медицини, забезпечення конфіденційності медичної інформації про пацієнтів;

- розробка та впровадження єдиних стандартів даних та забезпечення їх сумісності із національними реєстрами та європейськими медичними інформаційними системами та базами даних;

- розробка та впровадження дорожньої карти з розвитку цифрової інфраструктури, її масштабування, модернізації для забезпечення ефективності цифрових трансформацій та функціонування цифрової системи охорони здоров’я;

- трансформувати систему фінансового забезпечення функціонування цифрової системи охорони здоров’я;

- сформувати та запровадити інструменти щодо залучення, формування, розподілу, перерозподілу та використання фінансових ресурсів для здійснення процесів цифрової трансформації;

- розробити та запровадити етичні вимоги щодо використання технологій штучного інтелекту в медицині;

- розробка та реалізації інформаційної політики щодо популяризації та поширення інформації серед населення про цифрову трансформацію системи охорони здоров’я;

- розробка та запровадження заходів із навчання цифровим компетенціям медичного, управлінського та іншого персоналу системи охорони здоров’я;

- розробка та впровадження інструментів забезпечення рівного доступу населення до власних медичних даних через підвищення рівня їх цифрової компетенції;

- розробка інструментів державної підтримки розвитку інновацій в забезпеченні функціонування цифрової системи охорони здоров’я;

- розробка та запровадження механізмів моніторингу, контролю та оцінки результатів за процесами цифрової трансформації та функціонування цифрової системи охорони здоров’я.

- формування системи координації діяльності суб'єктів цифрової трансформації для забезпечення узгодженої взаємодії органів державної влади, органів місцевого самоврядування, закладів охорони здоров'я, IT-компаній, наукових установ та інститутів громадянського суспільства;

- організація міжнародного співробітництва з Європейським Союзом та країнами-членами Європейського Союзу;

- організація інформаційно-комунікаційної системи з відповідними органами Європейського Союзу щодо цифрової трансформації системи охорони здоров'я та відповідності вимогам інтеграції.

Зазначений перелік завдань є загальним та може змінюватися як в контексті розширення окремого завдання, так і в частині розширення усього переліку. Для забезпечення їх виконання трансформується методологія державного управління, що реалізується через сукупність принципів.

Важливою складовою методології державного управління, що визначає вплив суб'єкту на об'єкт, через реалізацію методологічної дії, виконання мети та завдань є механізми державного управління. Саме механізми визначають якими способами держава досягає керованості процесів цифрової трансформації системи охорони здоров'я та функціонування цифрової системи охорони здоров'я. З огляду на комплексність і полісуб'єктність досліджуваного об'єкта жоден окремий механізм не є самодостатнім, адже результативність та ефективність державного управління визначається синергією правового, організаційного, фінансового, кадрового та інформаційного механізмів. Кожен з механізмів реалізує певні завдання та нейтралізує відповідні властивості-загрози, або підсилює властивості-переваги. Зважаючи на вказане зміст механізмів державного управління цифровою трансформацією системи охорони здоров'я вбачаємо в наступному:

- *правовий механізм* – це процес формування, удосконалення, затвердження, зміни, перегляду та застосування сукупності нормативно-правових актів та інших юридичних засобів та процедур, які формують правове поле здійснення та стимулювання процесів цифрової трансформації та функціонування цифрової системи охорони здоров'я, встановлюючи умови обігу медичних даних, електронної взаємодії,

застосування телемедицини та технологій штучного інтелекту, визначають права, обов’язки, відповідальність суб’єктів, а також гарантують захист прав людини, персональних даних, медичної таємниці, встановлення кримінальної відповідальності за кіберзлочини у сфері медицини, неправомірне використання цифрових технологій, неправомірне розповсюдження медичних даних. Зміст механізму передбачає наступну сукупність дій: формування нормативно-правової бази цифрової трансформації; правове регулювання використання цифрових медичних технологій; визначення правового статусу цифрових медичних сервісів; регулювання використання технологій штучного інтелекту; забезпечення захисту персональних даних; правове регулювання електронної взаємодії; відповідальність суб'єктів реалізації медичних послуг та державного і місцевого управління; гармонізація законодавства із правом Європейського Союзу.

- *організаційний механізм* - сукупність інституційних та управлінських засобів, що визначають склад суб'єктів, розподіл повноважень і відповідальності, порядок їх взаємодії та координації, а також процедури планування, формування, реалізації, моніторингу, супроводу, коригування державно-управлінських рішень щодо процесів цифрової трансформації системи охорони здоров’я та функціонування цифрової системи охорони здоров’я. Організаційний механізм безпосередньо спирається на принципи організації (системності, інституційної визначеності та взаємодії, координованості, субсидіарності, розмежування повноважень) і забезпечує подолання фрагментарності й дублювання функцій. Реалізація зазначеного механізму має забезпечити: інституційне розмежування повноважень між центральними органами виконавчої влади, органами місцевого самоврядування, власником ЕСОЗ, закладами охорони здоров’я, розробниками цифрових технологій та

програмного забезпечення; створення міжвідомчих координаційних структур між суб'єктами реалізації державної політики в різних сферах суспільного життя (охорона здоров'я, економічного розвитку, фінансового забезпечення, цифрового суспільства); узгодження регіональних програм розвитку охорони здоров'я із загальнодержавною стратегією цифрової трансформації; організацію міжнародного співробітництва з Європейським Союзом для забезпечення сумісності цифрових систем; забезпечення безперервності управлінського циклу та організаційної адаптивності суб'єктів до змін, які виникають в результаті інноваційного розвитку цифрових технологій, медицини, управління; стандартизація процесів управління на різних рівнях, надання медичної допомоги; моніторинг та коригування реалізації державно-управлінських рішень.

- *інформаційний механізм* - сукупність засобів організації інформаційної взаємодії між суб'єктами державного управління, інформаційно-аналітичного забезпечення, супроводу управлінських процесів та обміну даними, необхідних для реалізації цифрової трансформації й ухвалення рішень на основі даних, що реалізуються через використання інформаційних ресурсів, інформаційно-аналітичних систем, цифрових платформ та інформаційних потоків. Реалізація інформаційного механізму відбувається в трьох напрямках: по-перше, формування інформаційного забезпечення та прогнозування для прийняття державно-управлінських рішень щодо цифрової трансформації системи охорони здоров'я; по-друге, популяризація цифрових сервісів, підвищення рівня суспільної довіри та забезпечення прийняття змін в суспільстві; по-третє, комунікація між зацікавленими сторонами для забезпечення інформаційної відкритості та прозорості державної політики.

- *кадровий механізм* - це сукупність управлінських заходів щодо формування, розвитку, професійної підготовки та ефективного

використання кадрового потенціалу, спрямованих на забезпечення необхідного рівня професійних і цифрових компетентностей медичних, управлінських та ІТ-фахівців, залучених до впровадження, використання й розвитку цифрових технологій, що необхідне для реалізації державної політики цифрової трансформації та функціонування цифрової системи охорони здоров’я. Ключовими напрямками розвитку кадрового механізму є: запровадження обов'язкових професійних стандартів цифрової компетентності; інтеграцію цифрових компетентностей в освітні програми закладів вищої освіти за медичними спеціальностями; впровадження системи безперервного професійного розвитку; запровадження етичного регулювання застосування технологій штучного інтелекту; впровадження заходів з адаптації персоналу й пацієнтів у гібридний період; формування цифрової культури.

- *фінансовий механізм* - це сукупність інструментів, джерел, методів та моделей залучення, формування, розподілу, перерозподілу та використання фінансових ресурсів держави, місцевого самоврядування, закладів охорони здоров'я, міжнародних донорів і приватного сектору, що визначають спроможність упроваджувати, підтримувати, масштабувати та модернізовувати цифрові технології та інфраструктуру в систему охорони здоров’я. Фінансовий механізм є матеріально-ресурсною основою реформи й фактично встановлює її параметри, адже навіть за наявності політичної волі саме фінансовий механізм визначає, чи отримають заклади ресурси на обладнання, програмне забезпечення й ліцензії. Даний механізм має забезпечити фінансування як етапу впровадження, так і безперервного, безпечного функціонування цифрової системи. В умовах війни та недостатності ресурсів є потреба розробки інструментів залучення грантової та міжнародної технічної допомоги, реалізації проєктів публічно-приватного партнерства. Важливою складовою фінансового

механізму є оцінювання економічної ефективності цифрової трансформації системи охорони здоров’я.

Таким чином, 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. Отже, обґрунтовано комплексний підхід до розуміння об’єкта державного управління цифровою трансформацією 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. 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.

Висновки до 2-го розділу

1. 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.

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. Визначені та згруповані властивості системи охорони здоров'я розширюють теоретичне наукове знання та формують методологічне підґрунтя державного управління цифровою трансформацією системи охорони здоров'я.

3. 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 до їх змісту. Для вирішення зазначеного розроблено багаторівневу структуру державного управління цифровою трансформацією та цифровою системою охорони здоров’я, зокрема: до стратегічних принципів (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) відносяться стратегічної спрямованості, людиноцентричності, євроінтеграційної орієнтованості, інноваційності, випереджувального розвитку, наукової обґрунтованості; до 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) відносяться системності, інституційної визначеності, інституційної взаємодії, координованості, субсидіарності, розмежування повноважень і відповідальності, підзвітності, компетентності, безперервності управлінського циклу, організаційної адаптивності; до принципів 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) відносяться інтероперабельності, даноцентричності, цифрової безперервності, простежуваності, інтелектуалізації, цифрової доступності, масштабованості, технологічної адаптивності; до принципів забезпечення (сукупність фундаментальних положень, які визначають правові, фінансово-економічні, кадрові, інформаційні та безпекові умови формування, функціонування і подальшого розвитку цифрової системи охорони здоров'я) відносяться законності, комплексної безпеки, ризик-орієнтованості, ресурсної достатності, кадрової спроможності, економічної доцільності, резервування та відновлюваності, контрольованості, етичності, соціальної інклюзивності.

4. 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.

5. 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. Отже, обґрунтовано комплексний підхід до розуміння об'єкта державного управління цифровою трансформацією 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.

6. 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.

РОЗДІЛ 3
СУЧАСНИЙ СТАН ТА НАСЛІДКИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я ЯК ОБ'ЄКТУ ДЕРЖАВНОГО УПРАВЛІННЯ

3.1. Світові тенденції цифрової трансформації системи охорони здоров'я

Стрімкий розвиток інформаційно-комунікаційних технологій, поширення електронних медичних записів, телемедицини, систем управління медичними даними, технологій штучного інтелекту та аналітики великих даних суттєво змінюють підходи до організації медичної допомоги, управління ресурсами галузі та взаємодії між державою, медичними працівниками і пацієнтами. У таких умовах цифровізація розглядається не лише як технологічний процес, а як комплексна управлінська трансформація, спрямована на підвищення ефективності функціонування систем охорони здоров'я, забезпечення доступності медичних послуг та покращення стану здоров'я населення. Цифрові технології дедалі більше впливають на якість і результативність медичної допомоги, формування доказової політики у сфері охорони здоров'я та забезпечення стійкості систем охорони здоров'я до сучасних викликів. Особливої значущості процеси цифрової трансформації набули після пандемії COVID-19, яка прискорила впровадження електронних сервісів, дистанційних медичних консультацій, цифрових платформ обміну медичними даними та інструментів підтримки прийняття клінічних і управлінських рішень.

На міжнародному рівні питання цифровізації охорони здоров'я перебувають у центрі уваги Всесвітньої організації охорони здоров'я, Організації економічного співробітництва та розвитку, Світового банку та інших міжнародних інституцій, які формують стратегічні засади розвитку цифрового здоров'я, розробляють стандарти цифрового врядування та здійснюють оцінювання рівня цифрової зрілості національних систем охорони здоров'я. Водночас світова практика свідчить про значну диференціацію між країнами щодо рівня розвитку цифрової інфраструктури, впровадження електронних медичних записів, використання телемедичних технологій, персональних медичних даних та штучного інтелекту в охороні здоров'я.

Дослідження сучасних світових тенденцій цифровізації систем охорони здоров'я та визначення ключових напрямів розвитку цифрового здоров'я в контексті підвищення ефективності функціонування національних систем охорони здоров'я передбачає вирішення нами таких завдань:

– проаналізувати стратегічні напрями розвитку цифрового здоров'я відповідно до Глобальної стратегії цифрового здоров'я ВООЗ 2020–2025;

– дослідити рівень цифрового розвитку держав та цифрової зрілості систем охорони здоров'я на основі індексів E-Government Development Index, Digital Health Index та Global Digital Health Monitor;

– оцінити рівень доступності електронних медичних записів та цифрової грамотності населення щодо використання цифрових медичних сервісів;

– проаналізувати масштаби поширення телемедичних технологій і визначити їх роль у забезпеченні доступності медичної допомоги;

– дослідити особливості розвитку систем персональних медичних даних та цифрових платформ взаємодії пацієнтів із системою охорони здоров'я у провідних країнах світу;

– визначити основні напрями впровадження технологій штучного інтелекту в систему охорони здоров'я та оцінити їх вплив на діяльність медичних працівників;

– проаналізувати рівень розвитку національних систем медичних даних і можливості використання великих масивів даних для моніторингу, наукових досліджень та підтримки управлінських рішень;

– охарактеризувати сучасні підходи до цифровізації громадського здоров'я як складової цифрової трансформації систем охорони здоров'я.

Реалізація поставлених завдань дозволяє комплексно оцінити сучасний стан та основні тенденції розвитку цифрового здоров'я у світі, визначити провідні міжнародні практики цифрової трансформації охорони здоров'я та сформувати наукове підґрунтя для подальшого дослідження європейського досвіду та особливостей цифровізації системи охорони здоров'я України.

У межах нашого дослідження поняття «цифрове здоров'я» використовується відповідно до термінології ВООЗ (Digital Health), тоді як поняття «цифровізація охорони здоров'я» та «цифрова трансформація охорони здоров'я» застосовуються для характеристики процесів впровадження цифрових технологій та їх впливу на функціонування систем охорони здоров'я.

Однією з ключових передумов глобальної цифрової трансформації охорони здоров'я стало затвердження Всесвітньою організацією охорони здоров'я Глобальної стратегії цифрового здоров'я на 2020–2025 роки (Global Strategy on Digital Health 2020–2025), яка визначила стратегічні орієнтири розвитку цифрових технологій у сфері охорони здоров'я на міжнародному

рівні. У документі підкреслюється, що цифрове здоров'я розглядається як важливий інструмент досягнення Цілей сталого розвитку, забезпечення загального охоплення населення медичними послугами та підвищення ефективності функціонування національних систем охорони здоров'я. Відповідно до бачення Стратегії, цифрове здоров'я повинно забезпечувати доступні, якісні, безпечні та орієнтовані на потреби людини медичні послуги шляхом використання цифрових технологій для профілактики захворювань, діагностики, лікування, реабілітації, паліативної допомоги та управління системою охорони здоров'я. Особлива увага приділяється забезпеченню безпеки та конфіденційності персональних медичних даних, розвитку цифрової інфраструктури та підвищенню рівня цифрової грамотності населення й медичних працівників.

Для досягнення визначених пріоритетів Глобальна стратегія цифрового здоров’я ВООЗ 2020–2025 формує комплексну систему взаємопов’язаних стратегічних цілей, реалізація яких забезпечує послідовний розвиток цифрової трансформації систем охорони здоров’я на міжнародному, національному та інституційному рівнях. Узагальнену характеристику цих стратегічних напрямів наведено на рис. 3.1.

На основі аналізу положень Глобальної стратегії цифрового здоров’я ВООЗ 2020–2025 встановлено, що сучасна цифрова трансформація системи охорони здоров’я виходить далеко за межі впровадження окремих інформаційно-комунікаційних технологій. Вона передбачає комплексну модернізацію механізмів публічного управління, яка охоплює удосконалення нормативно-правового забезпечення, інституційного розвитку, кадрового потенціалу, управління медичними даними та розвитку цифрової інфраструктури. У цьому контексті цифрові технології виступають не самостійною метою, а інструментом підвищення ефективності функціонування системи охорони здоров’я та забезпечення її стійкого розвитку.



Рис. 3.1. Стратегічна модель цифрової трансформації охорони здоров'я відповідно до Глобальної стратегії цифрового здоров'я ВООЗ 2020 - 2025 рр.

Джерело: складено автором на основі Global Strategy on Digital Health 2020–2025 *[165]*

Аналітична оцінка положень Глобальної стратегії цифрового здоров'я ВООЗ свідчить про формування нової управлінської парадигми, відповідно до якої цифрове здоров'я інтегрується у всі рівні державної політики та стає одним із ключових чинників забезпечення доступності, якості та безперервності медичної допомоги. Особливе значення має інституціоналізація цифрової трансформації через розроблення та реалізацію національних стратегій цифрового здоров'я, що забезпечує узгодженість державної політики, концентрацію ресурсів і довгострокове планування цифрових реформ.

Слід відзначити, що ефективність цифровізації безпосередньо залежить від створення єдиного інформаційного простору охорони здоров'я, заснованого на принципах стандартизації та інтероперабельності інформаційних систем. Це сприяє підвищенню якості управлінських рішень, оперативності обміну медичною інформацією та формуванню достовірної аналітичної бази для стратегічного планування розвитку галузі. У зв'язку з цим медичні дані поступово перетворюються на важливий стратегічний ресурс публічного управління, що потребує належного правового регулювання, гарантування конфіденційності, кібербезпеки та дотримання етичних стандартів їх використання.

Важливою тенденцією сучасного етапу розвитку цифрового здоров'я є інтеграція технологій штучного інтелекту, великих даних, цифрових медичних пристроїв та цифрових терапевтичних рішень у процеси управління системою охорони здоров'я. Їх використання відкриває нові можливості для прогнозування захворюваності, оптимізації розподілу ресурсів, підтримки клінічного прийняття рішень та персоналізації медичної допомоги, водночас актуалізуючи потребу у формуванні сучасних механізмів державного регулювання цифрових інновацій.

Проведений аналіз Глобальної стратегії цифрового здоров’я ВООЗ також засвідчує зміну концептуальних засад функціонування системи охорони здоров’я від технологічно орієнтованої до людиноцентричної моделі управління. У межах такого підходу пацієнт розглядається не лише як отримувач медичних послуг, а як активний учасник процесу управління власним здоров’ям, який має доступ до персональних медичних даних, цифрових сервісів та інструментів прийняття обґрунтованих рішень. Це відповідає сучасним принципам публічного управління, що базуються на відкритості, прозорості, сервісній орієнтації та підвищенні якості публічних послуг.

Вагомою передумовою розвитку цифрової трансформації охорони здоров'я є загальний рівень цифрового розвитку держави, який визначає можливості впровадження електронних сервісів, розвитку цифрової інфраструктури, забезпечення доступу населення до інформаційно-комунікаційних технологій та формування необхідних цифрових компетентностей. Одним із найбільш авторитетних міжнародних показників оцінювання цифрової зрілості державного сектору є Індекс розвитку електронного урядування ООН (UN E-Government Development Index, EGDI), який характеризує рівень розвитку цифрового врядування та готовність країн до впровадження цифрових публічних послуг. Рейтинг провідних країн світу за значенням E-Government Development Index у 2024 році наведено на рис. 3.2.

Дані рис. 3.2 свідчать, що у 2024 році найвищі значення Індексу розвитку електронного урядування продемонстрували Данія – 0,98, Естонія – 0,97, Сінгапур – 0,97, Республіка Корея – 0,97 та Ісландія – 0,97. Високі позиції зазначених країн зумовлені комплексним розвитком цифрових державних послуг, сучасної телекомунікаційної інфраструктури та високим рівнем цифрової грамотності населення.

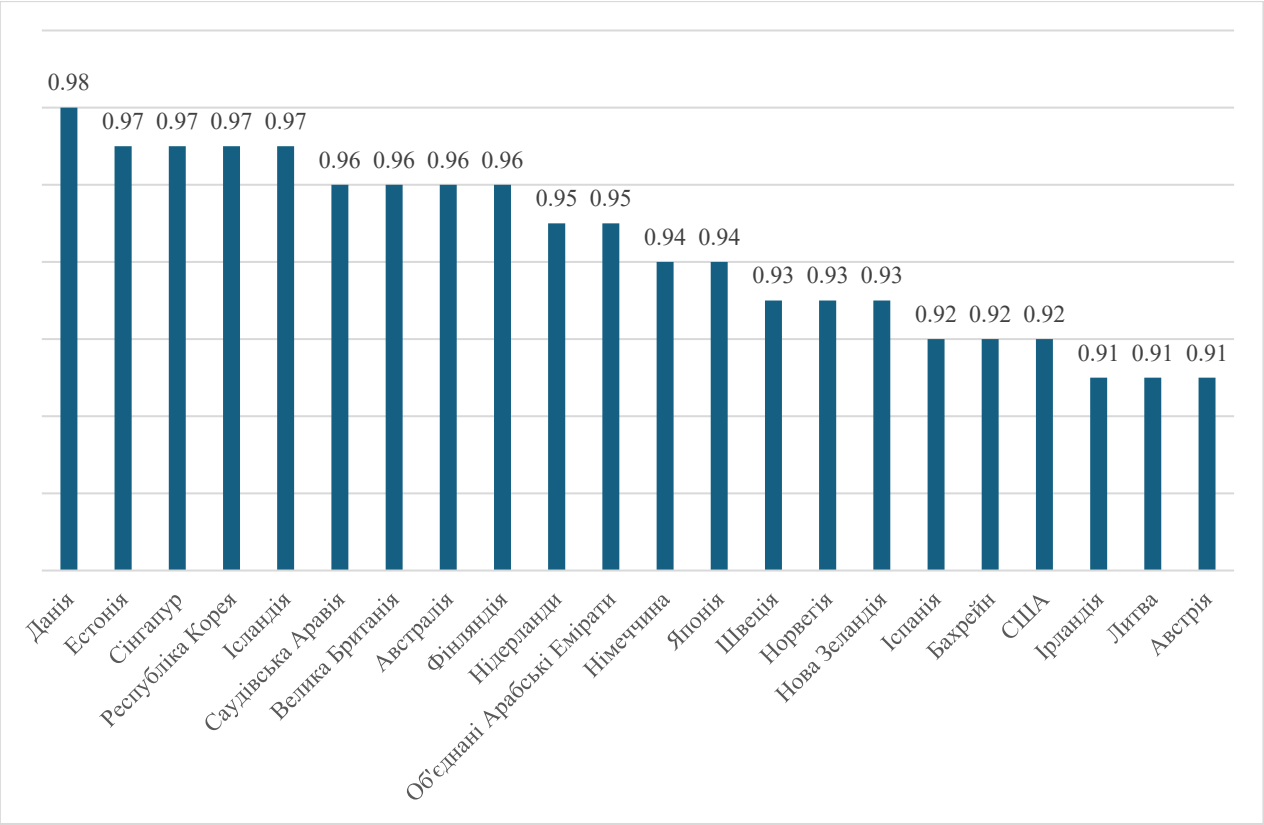


Рис. 3.2. Рейтинг країн за значенням E-Government Development Index, 2024 р. [279]

До групи держав із дуже високим рівнем цифрового розвитку також належать Саудівська Аравія, Велика Британія, Австралія, Фінляндія та Нідерланди, значення індексу яких перебуває в межах від 0,95 до 0,96. Водночас навіть країни, які посідають нижчі позиції серед представленої групи лідерів, зокрема Ірландія, Литва та Австрія, демонструють високі значення індексу на рівні 0,91.

Особливу увагу привертає Естонія, яка поряд із Данією залишається одним із світових лідерів цифрового врядування та водночас входить до числа найбільш цифрово розвинених систем охорони здоров'я у світі. Це підтверджує наявність тісного взаємозв'язку між загальним рівнем цифрової трансформації державного управління та успішністю впровадження цифрових технологій у сфері охорони здоров'я.

Пріоритетним індикатором розвитку цифрової трансформації систем охорони здоров'я є оцінювання рівня впровадження цифрових технологій та цифрових сервісів у медичній галузі. З цією метою в міжнародній практиці використовується Digital Health Index, який дозволяє комплексно оцінити рівень розвитку цифрового здоров'я на основі показників доступності електронних медичних сервісів, використання електронних медичних записів, телемедичних технологій, цифрової взаємодії пацієнтів із закладами охорони здоров'я та інтеграції медичних даних. Аналіз значень даного індексу дає змогу визначити країни-лідери цифрової трансформації охорони здоров'я та виявити основні тенденції розвитку цифрового здоров'я у світовому масштабі. Рейтинг країн за значенням Digital Health Index наведено на рис. 3.3.

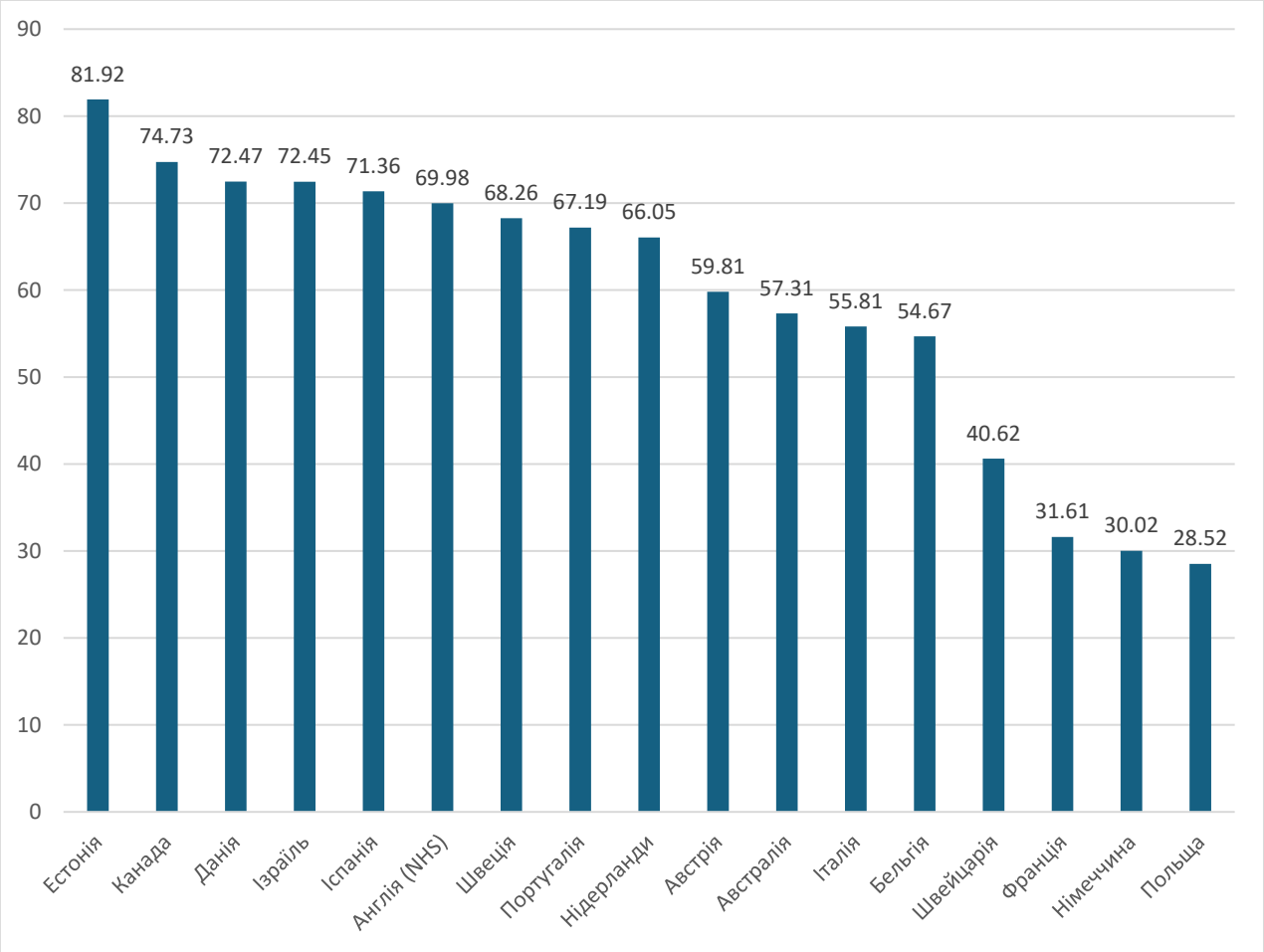


Рис. 3.3. Рейтинг країн за значенням Digital Health Index, 2025 [80]

Дані рис. 3.3 свідчать, що серед досліджуваних країн Digital Health Index 2025 абсолютним лідером рейтингу є Естонія, яка набрала 81,92 бала. Такий результат підтверджує високий рівень розвитку цифрового врядування та цифрової інфраструктури країни, що забезпечує повну інтеграцію електронних медичних записів, електронних рецептів та цифрових сервісів для населення. До групи країн із високим рівнем цифрового здоров'я також належать Канада (74,73 бала), Данія (72,47 бала), Ізраїль (72,45 бала) та Іспанія (71,36 бала). Високі позиції Данії, Швеції, Нідерландів та Англії свідчать про ефективність державної політики цифрової трансформації охорони здоров'я, спрямованої на розвиток електронних медичних записів, телемедицини та національних цифрових платформ управління медичними даними. Водночас країни Північної Європи демонструють найкращі результати щодо інтеграції медичних даних та забезпечення доступу громадян до цифрових медичних сервісів.

Середній рівень цифрової зрілості систем охорони здоров'я характерний для Австрії, Австралії, Італії та Бельгії, значення індексу яких коливається від 54 до 60 балів. Це свідчить про наявність розвиненої цифрової інфраструктури, проте одночасно вказує на необхідність подальшого вдосконалення механізмів інтеграції медичних даних та розширення цифрових сервісів для населення.

Найнижчі показники зафіксовано у Франції (31,61 бала), Німеччині (30,02 бала) та Польщі (28,52 бала). Незважаючи на високий рівень розвитку національних систем охорони здоров'я, ці країни демонструють нижчі темпи цифрової трансформації, що пов'язано з особливостями нормативно-правового регулювання, фрагментованістю інформаційних систем та складністю інтеграції цифрових медичних сервісів на національному рівні.

Для оцінювання практичних результатів реалізації Глобальної стратегії цифрового здоров'я ВООЗ ключовим є аналіз рівня цифрової зрілості національних систем охорони здоров'я. Одним із найбільш комплексних міжнародних інструментів оцінювання цифрової трансформації виступає Global Digital Health Monitor (GDHM), який здійснює моніторинг розвитку цифрового здоров'я за сімома ключовими напрямами: лідерство та врядування, стратегія та інвестиції, законодавство та політика, кадровий потенціал, стандарти, цифрова інфраструктура, цифрові сервіси та застосунки. Також важливим напрямом дослідження виступає інтероперабельність, тобто здатність різних інформаційних систем, програмного забезпечення, електронних сервісів і баз даних взаємодіяти між собою, обмінюватися інформацією та використовувати її без втрати змісту і необхідності додаткової обробки.

У наступній таблиці наведено узагальнені дані щодо оцінювання цифрової трансформації за даними Global Digital Health Monitor, 2024–2025 рр.

Таблиця 3.1

Порівняльна характеристика рівня цифрової зрілості систем охорони здоров'я за регіонами ВООЗ за даними Global Digital Health Monitor, 2024–2025 рр.

Регіон ВООЗ	Країни-лідери	Домінуюча фаза цифрової зрілості	Максимальна досягнута фаза
Африканський регіон	Ефіопія, Гвінея, Малаві, Танзанія	Фаза 2–3	Фаза 4
Панамериканський регіон	Бразилія, Чилі	Фаза 3–4	Фаза 4
Східно-Середземноморський регіон	Саудівська Аравія, ОАЕ	Фаза 2–4	Фаза 4
Регіон Західної частини Тихого океану	Малайзія, Філіппіни	Фаза 2–4	Фаза 4
Європейський регіон	Австрія*	Фаза 4	Фаза 4

Сформовано на основі [162]

Порівняльний аналіз регіональних даних Global Digital Health Monitor свідчить, що у всіх досліджуваних регіонах процес цифрової трансформації охорони здоров'я перебуває на етапі активного розвитку. Найбільш поширеними є друга, третя та четверта фази цифрової зрілості, тоді як країни п'ятої фази практично відсутні. Це підтверджує, що навіть держави-лідери цифрового здоров'я продовжують удосконалювати цифрові екосистеми охорони здоров'я.

Найвищі темпи цифрової трансформації демонструють країни, які реалізують комплексні державні стратегії цифрового здоров'я, інвестують у розвиток цифрової інфраструктури та забезпечують інтеграцію медичних інформаційних систем. Особливо це характерно для Саудівської Аравії, Об'єднаних Арабських Еміратів, Малайзії, Філіппін, Бразилії та Чилі. Водночас для більшості країн Африканського регіону характерним залишається етап формування базових інституційних та технологічних засад цифрового здоров'я.

Узагальнена оцінка цифрової зрілості дозволяє визначити загальний рівень розвитку цифрового здоров'я, проте не відображає особливостей розвитку окремих складових цифрової екосистеми. Для більш детального аналізу доцільно дослідити розподіл країн за доменами цифрової зрілості, представленими на рис. 3.4.

Отже, дані рис. 3.4 свідчать, що найбільш розвиненим напрямом цифрової трансформації є лідерство та врядування, де близько 54 % країн досягли четвертої та п'ятої фаз цифрової зрілості. Це вказує на формування в більшості держав належних управлінських механізмів, стратегічного бачення розвитку цифрового здоров'я та інституційної підтримки цифрових перетворень. Водночас лише незначна частка країн перебуває на початкових стадіях розвитку даного домену, що підтверджує усвідомлення урядами важливості цифровізації охорони здоров'я як одного з пріоритетних напрямів державної політики.

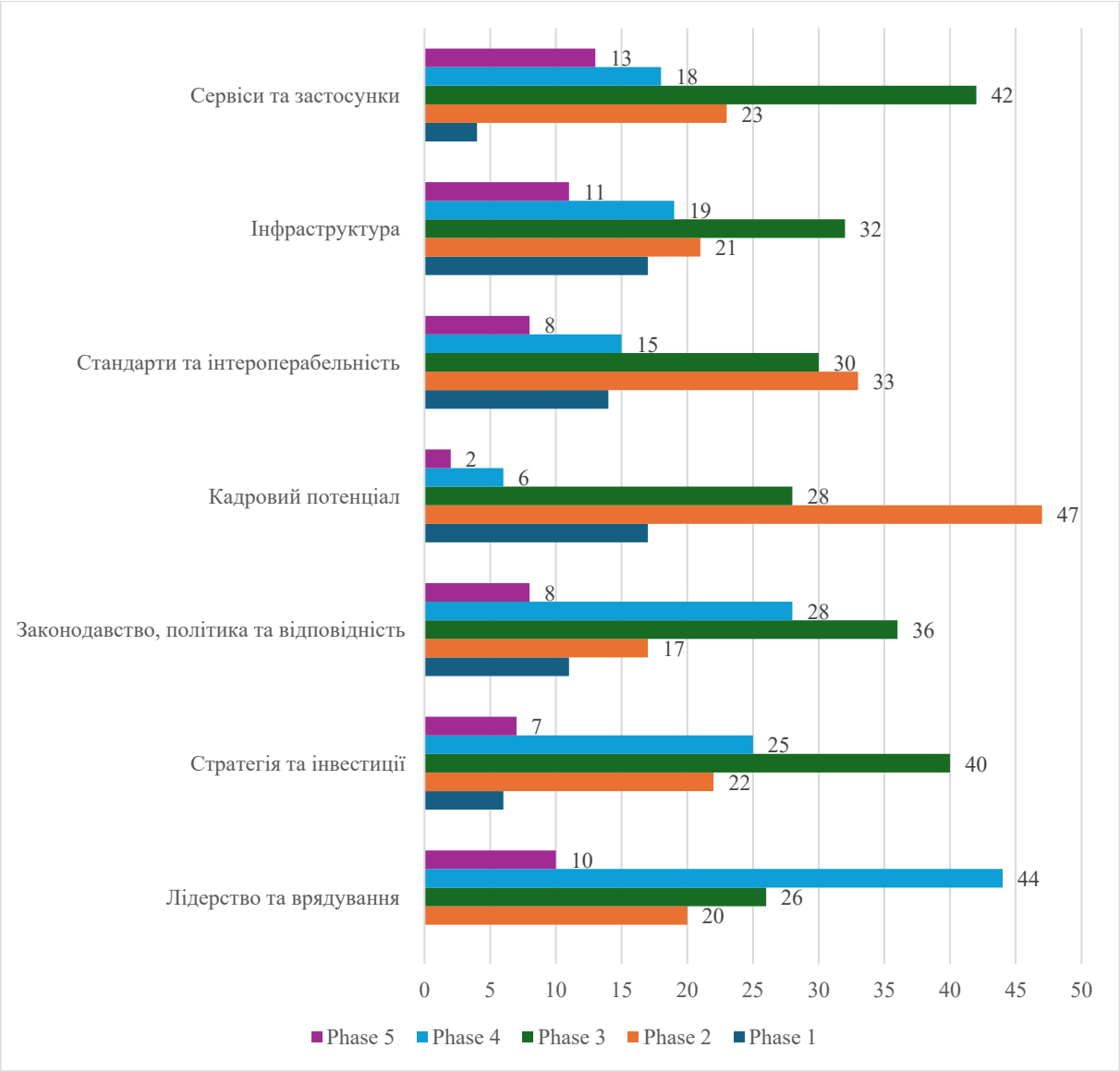


Рис. 3.4. Розподіл країн за фазами цифрової зрілості систем охорони здоров'я за основними доменами оцінювання у 2024 році, % [162]

Порівняно високий рівень розвитку спостерігається також у доменах стратегії та інвестицій, а також сервісів і застосунків. Майже дві третини країн досягли третьої або вищої фази зрілості, що свідчить про наявність національних стратегій цифрового здоров'я, поступове збільшення інвестицій у цифрову інфраструктуру та активне впровадження електронних медичних сервісів. Особливо значущим є той факт, що близько 73 % країн уже забезпечують функціонування цифрових сервісів

на рівні третьої фази зрілості або вище, що підтверджує глобальну тенденцію переходу від пілотних цифрових рішень до масштабного впровадження цифрових медичних послуг.

Середній рівень цифрової зрілості характерний для доменів законодавства, політики та відповідності, а також стандартів та інтероперабельності. Незважаючи на те, що більшість країн уже сформували базові нормативно-правові засади цифрового здоров'я, значна кількість держав все ще стикається з проблемами регулювання обігу медичних даних, забезпечення міждержавного обміну інформацією та впровадження механізмів регулювання штучного інтелекту в медицині. Крім того, недостатній розвиток інтероперабельності інформаційних систем обмежує можливості повноцінного обміну медичними даними між закладами охорони здоров'я та державними інформаційними ресурсами.

Особливу увагу привертає домен інфраструктури, у якому понад половина країн перебуває на третій та четвертій фазах розвитку. Це свідчить про активне нарощування цифрових потужностей, розширення мережевої готовності та розвиток інформаційно-комунікаційних технологій у сфері охорони здоров'я. Також майже половина держав ще не мають комплексних програм підтримки та модернізації цифрової інфраструктури, що стримує подальший розвиток цифрових медичних сервісів.

Найбільш проблемним напрямом цифрової трансформації залишається кадровий потенціал. Майже 65 % країн перебувають на першій та другій фазах цифрової зрілості у цьому домені, що свідчить про недостатній рівень підготовки фахівців, відсутність спеціалізованих освітніх програм та обмежені можливості професійного розвитку у сфері цифрового здоров'я. Низький рівень цифрових компетентностей медичних працівників є одним із головних факторів, що стримує ефективне впровадження цифрових технологій та уповільнює процес цифрової трансформації систем охорони здоров'я.

Таким чином, результати оцінювання цифрової зрілості засвідчують, що сучасний етап цифровізації охорони здоров'я у світі характеризується відносно високим рівнем розвитку управлінських механізмів, стратегічного планування та цифрових сервісів, водночас найбільш вразливими складовими залишаються кадрове забезпечення, інтероперабельність інформаційних систем та нормативно-правове регулювання новітніх цифрових технологій. Отримані результати підтверджують, що подальший розвиток цифрового здоров'я потребує комплексного підходу, спрямованого не лише на впровадження технологічних рішень, а й на розвиток людського капіталу, удосконалення системи управління та формування єдиного цифрового простору охорони здоров'я.

Високий рівень цифрової зрілості систем охорони здоров'я безпосередньо впливає на доступність цифрових медичних сервісів для населення. Одним із ключових показників людиноцентричної цифрової трансформації виступає забезпечення доступу громадян до електронних медичних записів, що відображено на рис. 3.5.

Проведений аналіз дає підстави стверджувати, що у більшості країн Європейського Союзу присутній високий рівень розвитку електронних медичних записів, що є одним із ключових показників цифрової трансформації охорони здоров'я та впровадження людиноцентричних підходів до надання медичних послуг. Забезпечення доступу громадян до власних медичних даних сприяє підвищенню прозорості медичного обслуговування, покращенню взаємодії між пацієнтами та закладами охорони здоров'я, а також створює передумови для розвитку персоналізованої медицини.

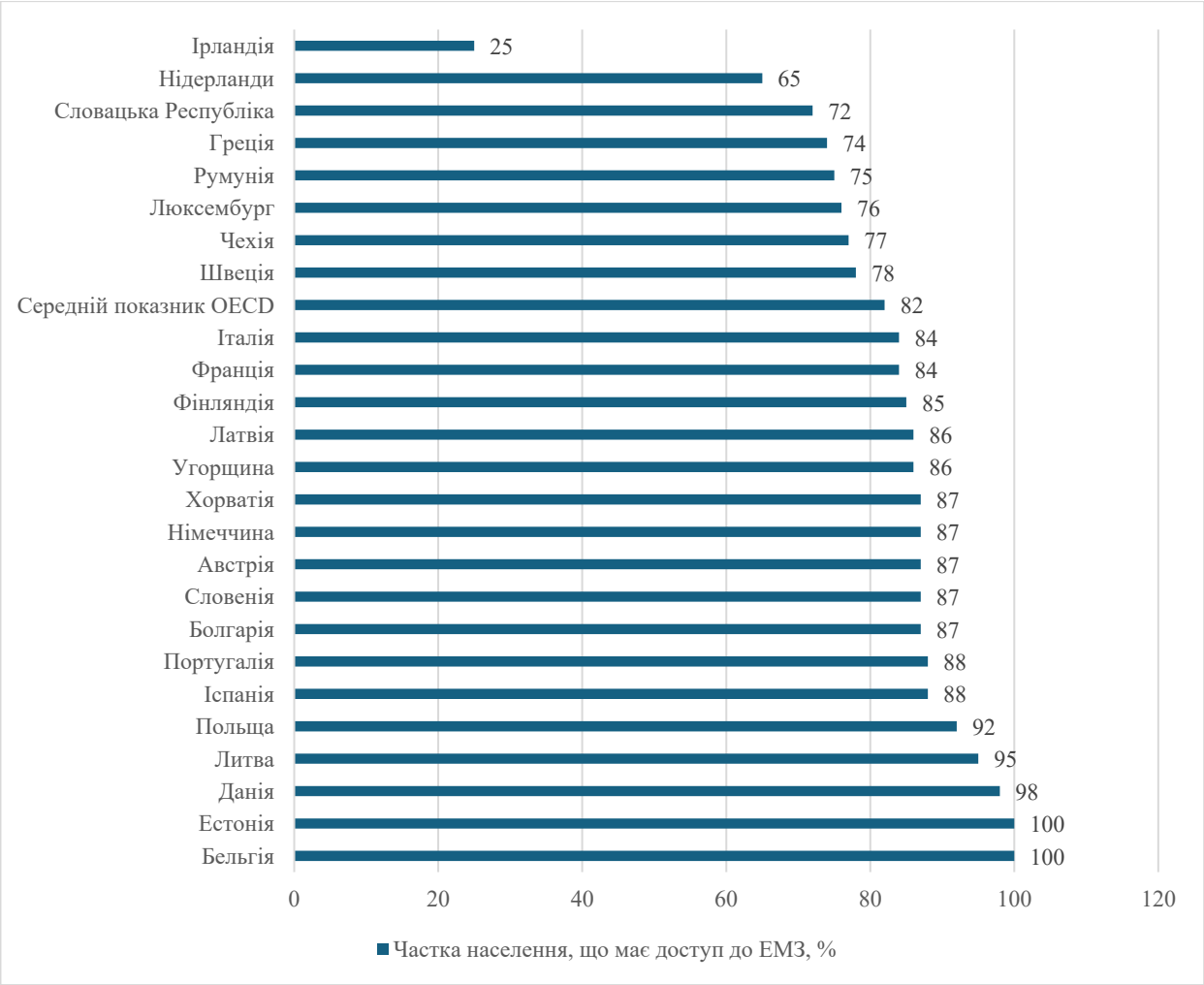


Рис. 3.5. Доступ населення до електронних медичних записів у країнах Європейського Союзу у 2024 році, % [226]

Найвищий рівень доступності електронних медичних записів зафіксовано у Бельгії та Данії, де доступ до ЕМЗ забезпечено для 100 % населення. До групи країн із високими показниками також належать Польща (98 %), Португалія (95 %), Словенія (88 %), Німеччина (87 %), Угорщина (87 %) та Фінляндія (86 %). Отримані результати свідчать про успішне впровадження національних цифрових платформ охорони здоров'я та високий рівень інтеграції електронних медичних сервісів у повсякденну медичну практику.

Середній рівень доступності електронних медичних записів характерний для Італії (84 %), Швеції (82 %), Люксембургу (77 %), Греції (72 %) та Нідерландів (65 %). Проте навіть у країнах із розвиненими системами охорони здоров'я спостерігаються відмінності щодо масштабів використання електронних медичних записів, що може бути пов'язано з особливостями організації національних інформаційних систем, нормативно-правового регулювання та рівнем цифрової активності населення.

Слід відзначити, що показник Ірландії, де доступ до електронних медичних записів мають лише 25 % населення, є найнижчим серед досліджуваних країн. Така ситуація свідчить про нерівномірність розвитку цифрових медичних сервісів навіть у межах Європейського Союзу та підтверджує необхідність подальшого вдосконалення механізмів цифрової трансформації охорони здоров'я.

Поряд із розвитком цифрової інфраструктури провідним фактором ефективного функціонування систем цифрового здоров'я є рівень цифрових компетентностей населення. Для оцінювання впливу освітнього чинника на використання цифрових медичних ресурсів доцільно проаналізувати показники цифрової грамотності населення, наведені на рис. 3.6.

У більшості досліджуваних країн особи з вищою освітою демонструють вищий рівень використання цифрових медичних ресурсів порівняно з населенням із нижчим рівнем освіти. Найвищі показники цифрової грамотності серед осіб із вищою освітою зафіксовано у Чехії (54 %), Уельсі (47 %), Франції (43 %), Австралії (39 %), США (36 %) та Канаді (33 %). Серед населення з нижчим рівнем освіти найвищі значення спостерігаються у Чехії (41 %), Уельсі (30 %), Саудівській Аравії (29 %), Франції (23 %) та Австралії (23 %).

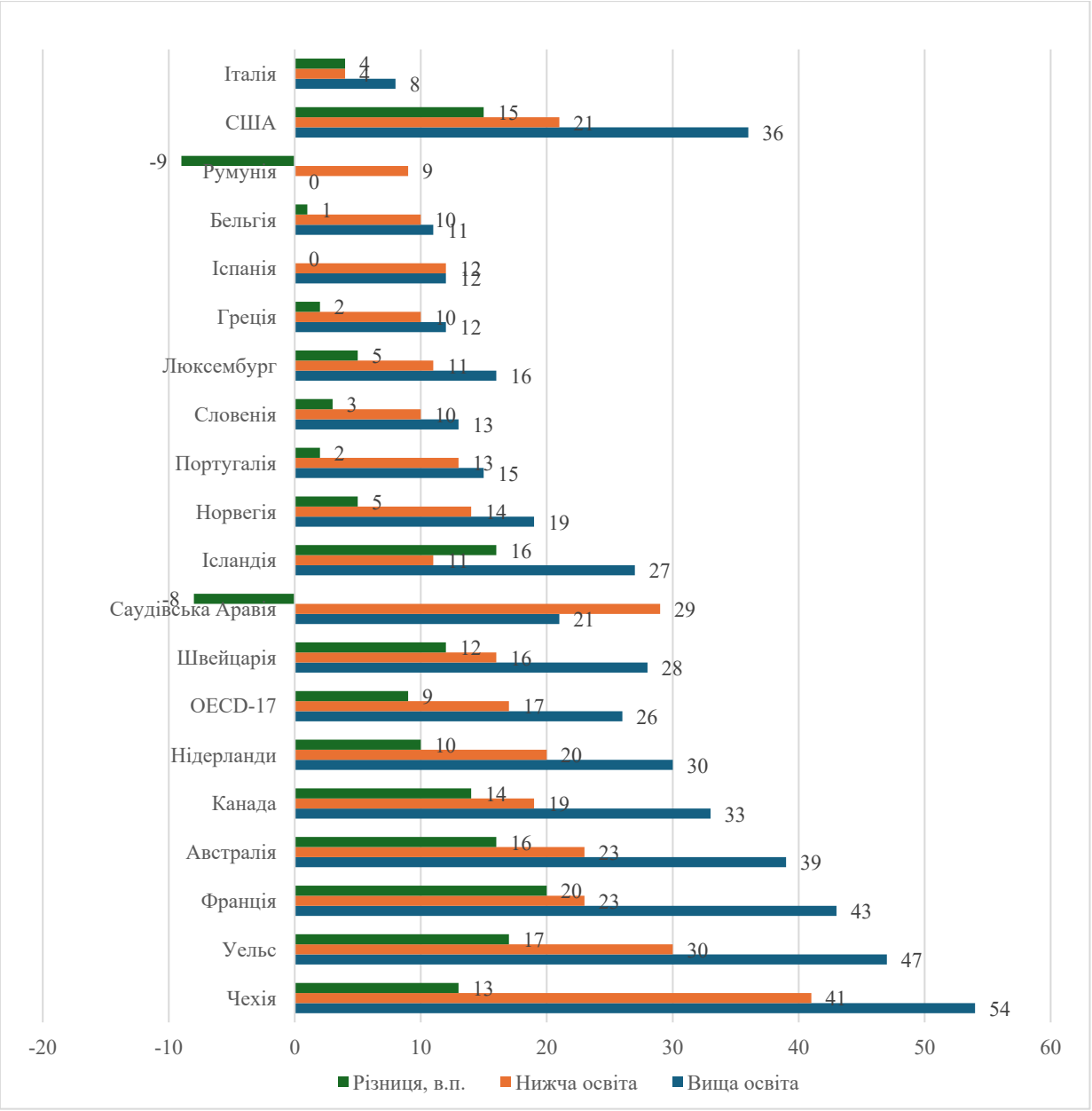


Рис. 3.6. Рівень цифрової грамотності у сфері охорони здоров'я залежно від рівня освіти населення у країнах OECD у 2024 році, % [226]

Найбільший розрив між освітніми групами виявлено у Франції (20 в.п.), Уельсі (17 в.п.), Австралії (16 в.п.), Ісландії (16 в.п.) та США (15 в.п.), що свідчить про значний вплив освітнього рівня на здатність населення використовувати цифрові інструменти охорони здоров'я. Водночас у Бельгії, Іспанії, Греції та Португалії різниця між групами є незначною та не перевищує декількох відсоткових пунктів.

Слід відзначити, що в Саудівській Аравії та Румунії показники цифрової грамотності серед населення з нижчим рівнем освіти перевищують відповідні значення серед осіб із вищою освітою. Це може свідчити про особливості національної структури вибірки, специфіку використання цифрових медичних сервісів або відмінності в соціально-демографічних характеристиках респондентів.

У середньому для країн Організації економічного співробітництва та розвитку (OECD-17) рівень цифрової грамотності становить 26 % серед осіб із вищою освітою та 17 % серед населення з нижчим рівнем освіти, що відповідає розриву у 9 відсоткових пунктів. Отримані результати підтверджують, що підвищення цифрових компетентностей населення є важливою умовою ефективного використання цифрових медичних сервісів та успішної цифрової трансформації систем охорони здоров’я.

Практичним проявом розвитку цифрового здоров'я є впровадження телемедичних технологій, які забезпечують дистанційне надання медичних послуг. Динаміка використання телемедичних консультацій у країнах Організації економічного співробітництва та розвитку наведена на рис. 3.7.

Результати аналізу телемедичних консультацій у країнах OECD свідчать про суттєве прискорення цифрової трансформації систем охорони здоров'я під впливом пандемії COVID-19. Якщо у 2019 році дистанційні консультації лікарів мали обмежене поширення та використовувалися переважно як додатковий інструмент надання медичної допомоги, то у період пандемії телемедицина стала одним із ключових механізмів забезпечення безперервності медичного обслуговування населення. За даними OECD, середня кількість телемедичних консультацій у країнах Організації зросла з 0,5 консультації на одну особу у 2019 році до 1,3 консультації у 2021 році, тобто більш ніж у 2,5 раза. У 2023 році показник дещо знизився до близько 1 консультації на особу, проте залишився майже удвічі вищим за допандемічний рівень.

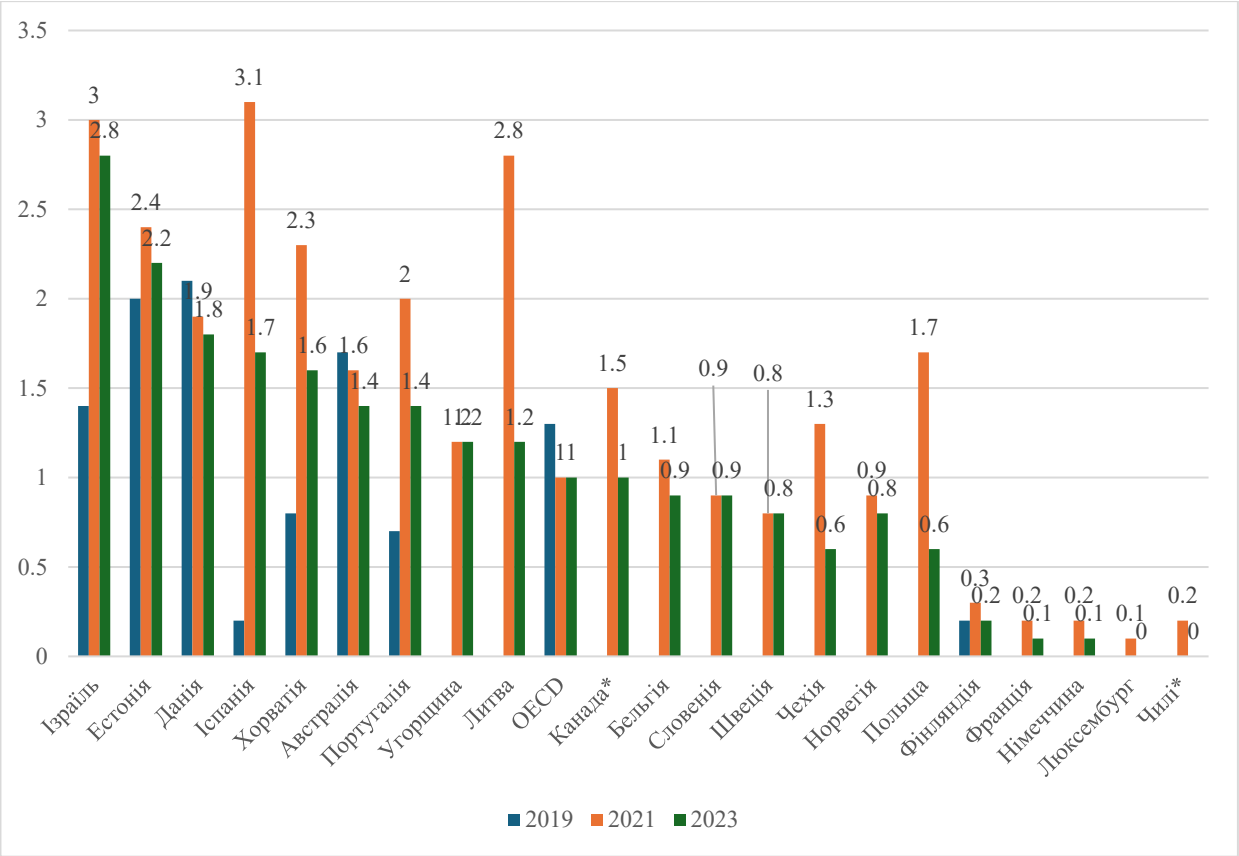


Рис. 3.7. Кількість телемедичних консультацій на одну особу в країнах OECD у 2019–2023 роках [226]

Найвищі показники використання телемедицини у 2023 році зафіксовано в Ізраїлі (2,8 консультації на одну особу), Естонії (2,2), Данії (1,8), Іспанії (1,7) та Хорватії (1,6). Високий рівень використання дистанційних консультацій у зазначених країнах свідчить про успішну інтеграцію цифрових сервісів у систему надання медичної допомоги та їх закріплення як повноцінного елементу сучасної медичної практики. Особливо показовим є приклад Ізраїлю, який протягом усього досліджуваного періоду демонструє найвищі показники використання телемедичних технологій серед країн OECD.

Найбільш динамічне зростання телемедичних консультацій у період пандемії спостерігалося в Іспанії та Литві. Зокрема, в Іспанії кількість дистанційних консультацій збільшилася з 0,2 у 2019 році до 3,1 у 2021 році,

що стало одним із найвищих показників серед усіх досліджуваних країн. Водночас після завершення пандемії в цих державах спостерігалося певне скорочення використання телемедичних сервісів, однак рівень їх застосування залишився значно вищим порівняно з допандемічним періодом. Подібна тенденція підтверджує перехід телемедицини від тимчасового кризового інструменту до постійного елемента системи охорони здоров'я.

Разом із тим аналіз демонструє значну диференціацію між країнами щодо рівня використання дистанційних консультацій. У Франції, Німеччині, Люксембурзі та Чилі кількість телемедичних консультацій у 2023 році не перевищувала 0,1–0,2 консультації на одну особу. Такі результати можуть бути пов'язані з особливостями організації національних систем охорони здоров'я, механізмами фінансування телемедичних послуг, рівнем цифрової інфраструктури та ступенем нормативно-правового врегулювання дистанційного медичного обслуговування.

Узагальнення наведених даних показує, що розвиток телемедицини має значне стратегічне значення, оскільки сприяє підвищенню доступності медичних послуг, особливо для населення віддалених територій, осіб з обмеженою мобільністю та пацієнтів із хронічними захворюваннями. Крім того, використання телемедичних технологій дозволяє оптимізувати навантаження на медичні заклади, скоротити витрати часу на отримання консультацій та забезпечити більш ефективне використання кадрових ресурсів системи охорони здоров'я.

Подальший розвиток цифрової охорони здоров'я пов'язаний із розширенням доступу громадян до персональних медичних даних. З цією метою провідні країни OECD впроваджують різні моделі пацієнтських порталів та персональних медичних записів, характеристику яких наведено у табл. 3.2.

Таблиця 3.2

Підходи до забезпечення доступу пацієнтів до персональних медичних даних у провідних країнах OECD

Країна	Портал пацієнта	Patient-accessible EHR (PaEHR)	Personal Health Record (PHR)
Австралія (My Health Record)	Так	Розробляється	Так
Данія (Sundhed.dk)	Так	Так	Ні
Фінляндія (MyKanta)	Так	Так	Розробляється
Японія (MynaPortal)	Так	Ні	Так
Велика Британія (NHS App, Англія)	Так	Розробляється	Розробляється

Джерело: складено автором за даними OECD Personal Health Data Systems in OECD Countries [226].

Аналіз практик п'яти провідних країн OECD демонструє, що всі досліджувані держави вже впровадили національні портали пацієнтів, які забезпечують громадянам доступ до власних медичних даних. Найбільш комплексні моделі сформовані в Данії та Фінляндії, де функціонують як портали пацієнтів, так і системи відкритого доступу до електронних медичних записів (Patient-accessible Electronic Health Records). Данська платформа Sundhed.dk забезпечує практично повний доступ громадян до медичних даних у режимі реального часу, тоді як фінська система MyKanta інтегрує інформацію з усіх рівнів надання медичної допомоги в межах єдиної національної інфраструктури.

Також вдало впроваджена австралійська модель My Health Record, яка базується на національній платформі персональних медичних даних та активно розвиває інструменти персоналізованого управління медичною інформацією. Також Японія реалізує цифрову трансформацію через платформу MynaPortal, інтегровану із загальнонаціональною стратегією цифрової трансформації охорони здоров'я. У Великій Британії цифровізація відбувається через застосунок NHS App, який поступово трансформується у повноцінну платформу персонального медичного запису.

Отже, під час аналізу виявлено, що провідною світовою тенденцією є поступовий перехід від традиційних електронних медичних записів до інтегрованих пацієнтоорієнтованих платформ управління персональними медичними даними, які забезпечують активну участь громадян у процесі управління власним здоров'ям.

У сучасних умовах цифрової трансформації охорони здоров'я особливого значення набуває впровадження технологій штучного інтелекту (Artificial Intelligence, AI), які формують новий етап розвитку медичних інформаційних систем та механізмів надання медичної допомоги. На відміну від традиційних цифрових інструментів, штучний інтелект забезпечує автоматизований аналіз великих масивів медичних даних, підтримку клінічного прийняття рішень, прогнозування перебігу захворювань, персоналізацію лікування та оптимізацію управлінських процесів у сфері охорони здоров'я. За оцінками OECD, впровадження AI здатне підвищити продуктивність медичних працівників, зменшити адміністративне навантаження на персонал та частково компенсувати дефіцит кадрів, який спостерігається у більшості країн світу. При цьому поширення технологій штучного інтелекту супроводжується низкою викликів, пов'язаних із захистом персональних даних, етичними аспектами використання алгоритмів, питаннями відповідальності за прийняті рішення та необхідністю формування нових цифрових компетентностей медичних працівників. У зв'язку з цим доцільним є дослідження сучасних напрямів використання штучного інтелекту в охороні здоров'я, аналіз його переваг і ризиків, а також оцінювання впливу AI на трансформацію кадрового потенціалу та розвиток цифрової екосистеми охорони здоров'я (рис. 3.8).

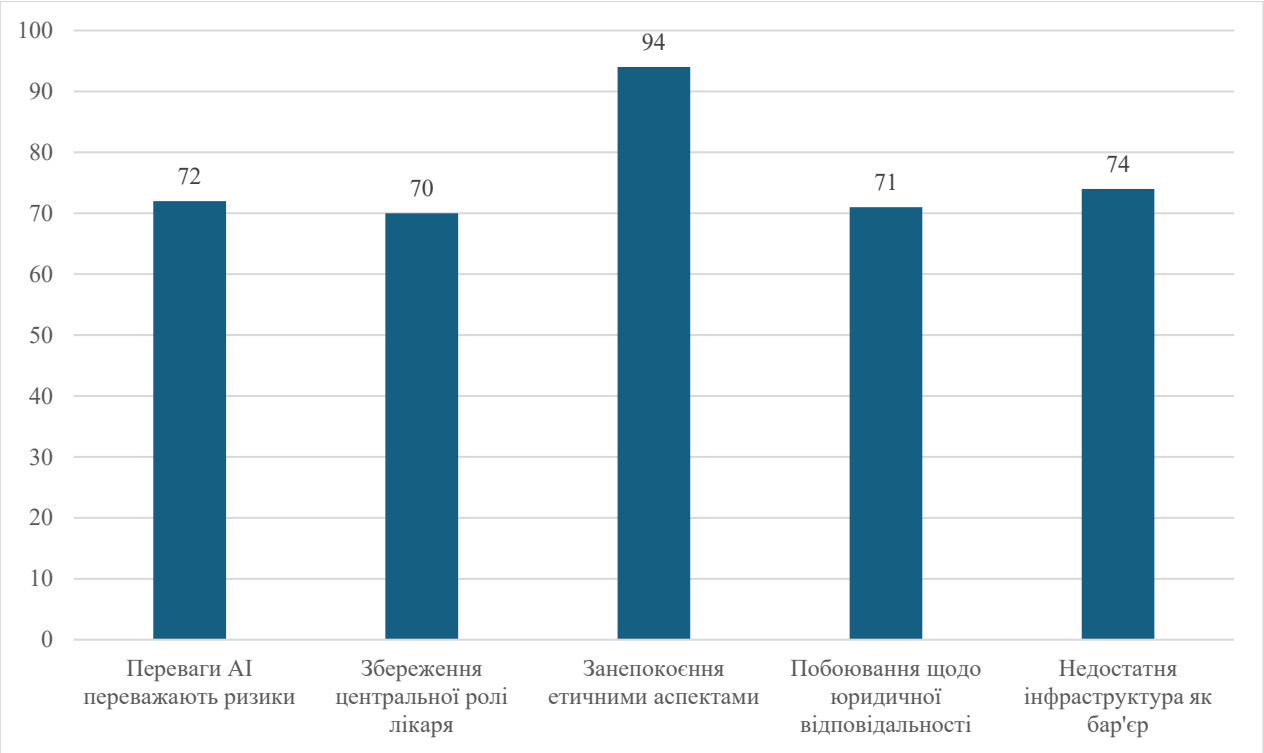


Рис. 3.8. Оцінка медичними асоціаціями наслідків впровадження штучного інтелекту в охорону здоров'я, % [90]

Результати опитування медичних асоціацій, проведеного OECD у 2024 році, свідчать загалом про позитивне ставлення професійної медичної спільноти до впровадження технологій штучного інтелекту в систему охорони здоров'я. Так, 72 % респондентів вважають, що потенційні переваги використання AI перевищують можливі ризики. Водночас медична спільнота демонструє збалансований підхід до цифрової трансформації галузі, акцентуючи увагу на необхідності належного регулювання та контролю таких технологій. Найвищий рівень занепокоєння пов'язаний з етичними аспектами застосування AI (94 % опитаних), а також питаннями професійної відповідальності медичних працівників за рішення, прийняті із залученням алгоритмів штучного інтелекту (71 %). Крім того, 74 % респондентів визначили недостатній рівень розвитку цифрової інфраструктури та доступності якісних даних як один із ключових бар'єрів для масштабного впровадження AI у медичну

практику. Водночас 70 % опитаних переконані, що навіть за умов стрімкого розвитку штучного інтелекту центральна роль лікаря в процесі надання медичної допомоги збережеться.

Поряд із розвитком електронних медичних записів, телемедичних сервісів та персональних медичних платформ важливим компонентом цифрової трансформації охорони здоров'я є формування національних систем медичних даних. Ефективність сучасної системи цифрового здоров'я значною мірою залежить від повноти охоплення населення медичними даними, рівня стандартизації інформації, використання унікальних ідентифікаторів пацієнтів, автоматизованого збору даних з електронних медичних записів та можливостей їх подальшого використання для моніторингу, наукових досліджень і прийняття управлінських рішень. З метою оцінювання рівня розвитку національних систем медичних даних у провідних країнах світу доцільно проаналізувати показники їх доступності, зрілості та практичного використання (рис. 3.9).

Отже, абсолютним лідером серед досліджуваних країн є Данія, яка демонструє максимальні значення за всіма показниками (100 %). Це свідчить про повністю інтегровану цифрову екосистему охорони здоров’я, що забезпечує ефективне управління медичними даними, їх стандартизацію та широке використання для прийняття управлінських рішень.

Високий рівень цифрової зрілості також характерний для Кореї та Швеції. У цих країнах практично всі ключові набори медичних даних охоплюють понад 90 % населення, використовуються стандартизовані клінічні термінології та унікальні ідентифікатори пацієнтів. Особливо важливо, що понад 90 % доступних даних застосовуються для моніторингу якості медичної допомоги, що свідчить про їх активне використання у процесах управління та планування розвитку системи охорони здоров’я.

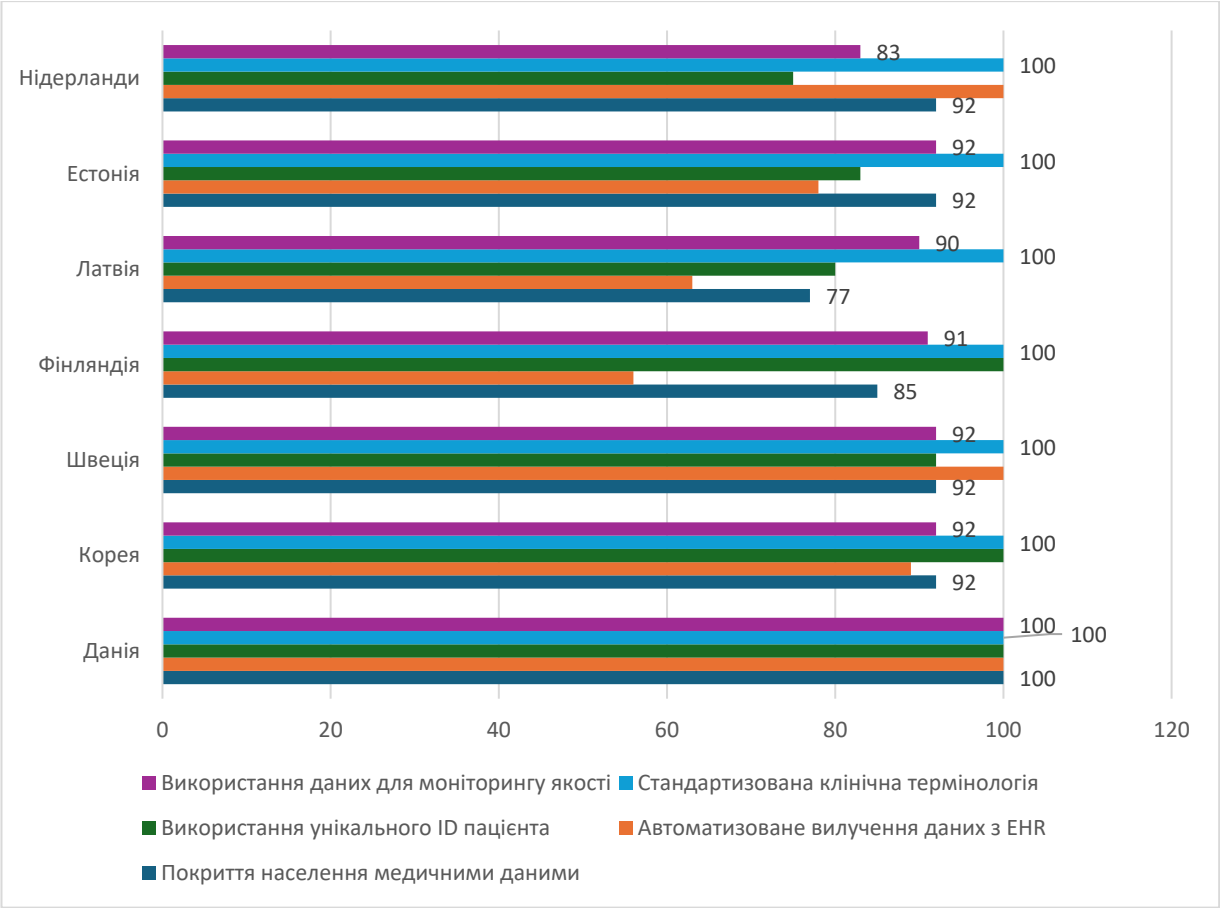


Рис. 3.9. Порівняльна характеристика доступності, зрілості та використання національних медичних даних у країнах OECD, 2019–2020 рр. [224]

Фінляндія та Нідерланди також демонструють високі показники цифрового розвитку. У Фінляндії рівень використання даних для моніторингу становить 91 %, а стандартизована клінічна термінологія та унікальний ідентифікатор пацієнта використовуються у 100 % випадків. Водночас показник автоматизованого вилучення даних з EHR складає лише 56 %, що свідчить про наявність потенціалу для подальшої автоматизації обробки медичної інформації. У Нідерландах аналогічний показник становить 83 %, що є одним із найвищих серед досліджуваних держав.

Суттєвий прогрес у цифровізації демонструють Естонія та Латвія, які традиційно належать до групи найбільш цифровізованих держав Європи. В Естонії показник використання унікального ідентифікатора пацієнта становить 83 %, а використання медичних даних для моніторингу – 92 %. У Латвії всі ключові набори даних доступні на національному рівні, однак рівень їх використання для моніторингу дещо нижчий і становить 90 %, а автоматизоване вилучення даних з електронних медичних записів – 63 %.

Рівень цифровізації систем охорони здоров'я визначається не лише наявністю медичних даних, а й ефективністю їх використання для управління галуззю, статистичного аналізу та наукових досліджень. Аналіз показує значні відмінності між країнами щодо доступності національних медичних наборів даних та рівня їх практичного застосування.

Отримані результати підтверджують, що високий рівень зрілості національних систем медичних даних створює інформаційну основу для прийняття доказових управлінських рішень, стратегічного планування розвитку системи охорони здоров'я та підвищення ефективності державної політики у сфері громадського здоров'я. У зв'язку з цим особливого значення набуває дослідження цифровізації громадського здоров'я як нового напряму цифрової трансформації медичної галузі, концептуальну основу якого представлено на рис. 3.10.

Найвищий рівень інтеграції медичних даних у процеси моніторингу та досліджень демонструють Данія, Канада та Фінляндія, де 100 % доступних наборів даних регулярно використовуються для оцінювання функціонування системи охорони здоров'я. Такі результати свідчать про високий рівень розвитку цифрової інфраструктури, стандартизації даних та міжвідомчої взаємодії.

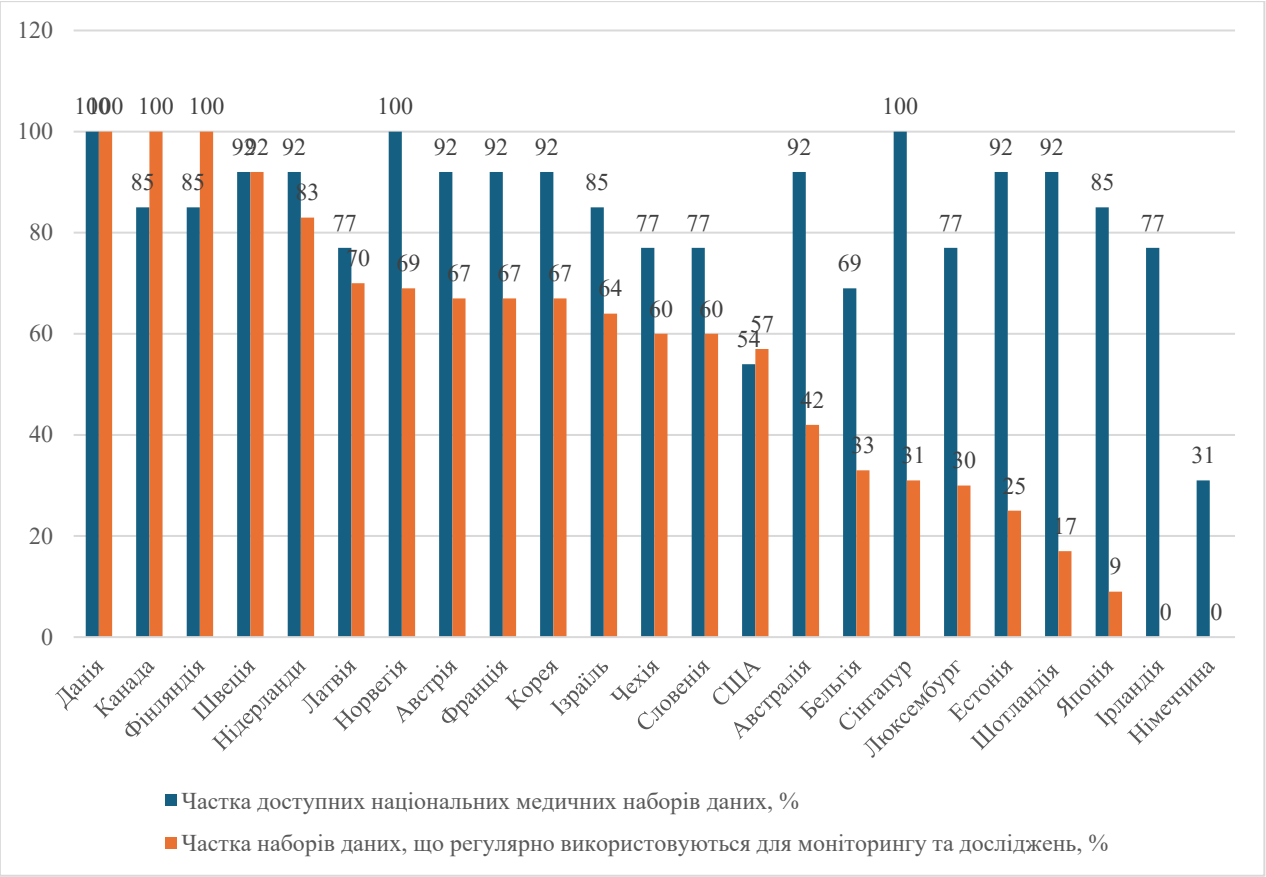


Рис. 3.10. Доступність ключових національних медичних наборів даних та їх використання для моніторингу і наукових досліджень у країнах OECD, % [224]

До групи країн із високими показниками також належать Швеція (92 %), Нідерланди (83 %), Латвія (70 %) та Норвегія (69 %). Спільною рисою цих держав є функціонування національних платформ медичних даних, використання електронних медичних записів та впровадження єдиних стандартів обміну інформацією.

Також у низці економічно розвинених країн спостерігається суттєвий розрив між доступністю даних та їх практичним використанням. Наприклад, у Сінгапурі доступними є 100 % ключових наборів даних, однак лише 31 % із них регулярно застосовуються для моніторингу та досліджень. Аналогічна ситуація характерна для Естонії (92 % і 25 % відповідно), Японії (85 % і 9 %) та Шотландії (92 % і 17 %).

Найнижчі показники зафіксовані в Німеччині та Ірландії, де регулярне використання медичних даних для досліджень фактично відсутнє. Це свідчить про наявність організаційних, правових або технічних бар'єрів щодо вторинного використання медичної інформації.

Отже, проведене дослідження дозволило встановити, що сучасний розвиток систем охорони здоров'я характеризується переходом від впровадження окремих цифрових технологій до формування комплексних цифрових екосистем, заснованих на інтегрованому використанні електронних медичних записів, телемедицини, персональних медичних даних, технологій штучного інтелекту, великих масивів даних та цифрових інструментів громадського здоров'я.

Аналіз Глобальної стратегії цифрового здоров'я ВООЗ 2020–2025 засвідчив, що ключовими напрямами цифрової трансформації охорони здоров'я є розвиток цифрового врядування, удосконалення національних стратегій цифрового здоров'я, забезпечення інтероперабельності інформаційних систем, розвиток цифрової інфраструктури та впровадження людиноцентричних підходів до надання медичної допомоги.

Результати дослідження міжнародних індексів підтвердили взаємозв'язок між загальним рівнем цифрового розвитку держави та рівнем цифрової трансформації системи охорони здоров'я. Лідерами за показниками E-Government Development Index у 2024 році стали Данія, Естонія, Сінгапур та Республіка Корея, тоді як найвищі значення Digital Health Index зафіксовано в Естонії, Канаді, Данії та Ізраїлі. Це свідчить про визначальну роль цифрового врядування, цифрової інфраструктури та державної політики у розвитку цифрового здоров'я.

Встановлено, що більшість країн світу перебуває на середньому та високому рівнях цифрової зрілості систем охорони здоров'я, проте найменш розвиненим напрямом залишається кадровий потенціал, що свідчить про необхідність подальшого розвитку цифрових

компетентностей медичних працівників. Важливим показником людиноцентричної цифрової трансформації є доступність електронних медичних записів, рівень якої у більшості країн Європейського Союзу перевищує 80 %, а в окремих державах охоплює практично все населення.

Дослідження цифрової грамотності населення підтвердило наявність стійкого взаємозв'язку між освітнім рівнем громадян та їх здатністю використовувати цифрові медичні сервіси. У середньому для країн OECD-17 різниця між особами з вищою та нижчою освітою становить 9 відсоткових пунктів, що свідчить про збереження цифрової нерівності та необхідність розвитку цифрової інклюзії.

Виявлено, що телемедицина стала одним із найбільш динамічних напрямів цифрової трансформації охорони здоров'я, забезпечуючи розширення доступу населення до медичних послуг незалежно від місця проживання. Водночас провідні країни світу переходять від традиційних електронних медичних записів до інтегрованих систем персональних медичних даних і національних пацієнтських порталів, що сприяє активному залученню громадян до управління власним здоров'ям.

Результати дослідження також засвідчили зростання ролі штучного інтелекту та великих масивів медичних даних у підтримці клінічних і управлінських рішень. Переважна більшість професійних медичних асоціацій визнає потенціал штучного інтелекту щодо підвищення ефективності медичної допомоги, водночас наголошуючи на необхідності вирішення етичних, правових та інфраструктурних питань його впровадження.

Таким чином, світовий досвід свідчить про формування нової цифрової моделі охорони здоров'я, у центрі якої перебувають дані, цифрові технології та пацієнт. Враховуючи високий рівень цифрового розвитку країн Європейського Союзу, доцільним є подальше дослідження європейського досвіду цифрової трансформації охорони здоров'я та можливостей його адаптації в Україні.

3.2. Сучасний стан та тенденції цифрової трансформації систем охорони здоров'я європейських країн

Поглиблення аналізу світових тенденцій цифровізації охорони здоров’я зумовлює необхідність дослідження особливостей розвитку цифрового здоров’я в європейських країнах. Європейський Союз посідає провідні позиції у формуванні сучасної цифрової політики у сфері охорони здоров’я, реалізуючи комплексний підхід до розвитку цифрової інфраструктури, забезпечення доступності медичних даних, впровадження транскордонних електронних сервісів та створення єдиного цифрового простору охорони здоров’я.

Особливістю європейської моделі цифрової трансформації є поєднання технологічних інновацій із високим рівнем нормативно-правового регулювання, захисту персональних даних, інтероперабельності інформаційних систем та орієнтації на потреби громадян. У межах реалізації стратегічних цілей Європейського Союзу здійснюється послідовний розвиток електронних медичних записів, цифрових платформ взаємодії пацієнтів і медичних працівників, телемедичних сервісів, а також механізмів транскордонного обміну медичною інформацією. У зв’язку з цим доцільним є дослідження рівня цифрового розвитку країн Європи, стану впровадження електронних медичних записів, особливостей функціонування Європейського простору даних охорони здоров’я, поширення телемедичних технологій та використання інноваційних цифрових рішень у медичній сфері. Такий аналіз дозволяє визначити ключові тенденції цифрової трансформації європейських систем охорони здоров’я та окреслити перспективні напрями їх подальшого розвитку.

Для оцінювання рівня цифрової готовності європейських країн до впровадження інноваційних рішень у сфері охорони здоров'я важливим є аналіз індексу цифрової економіки та суспільства (Digital Economy and Society Index –

DESI). Цей показник комплексно характеризує рівень цифрового розвитку держав за чотирма основними напрямами: людський капітал, цифрова інфраструктура, інтеграція цифрових технологій та цифрові державні послуги.

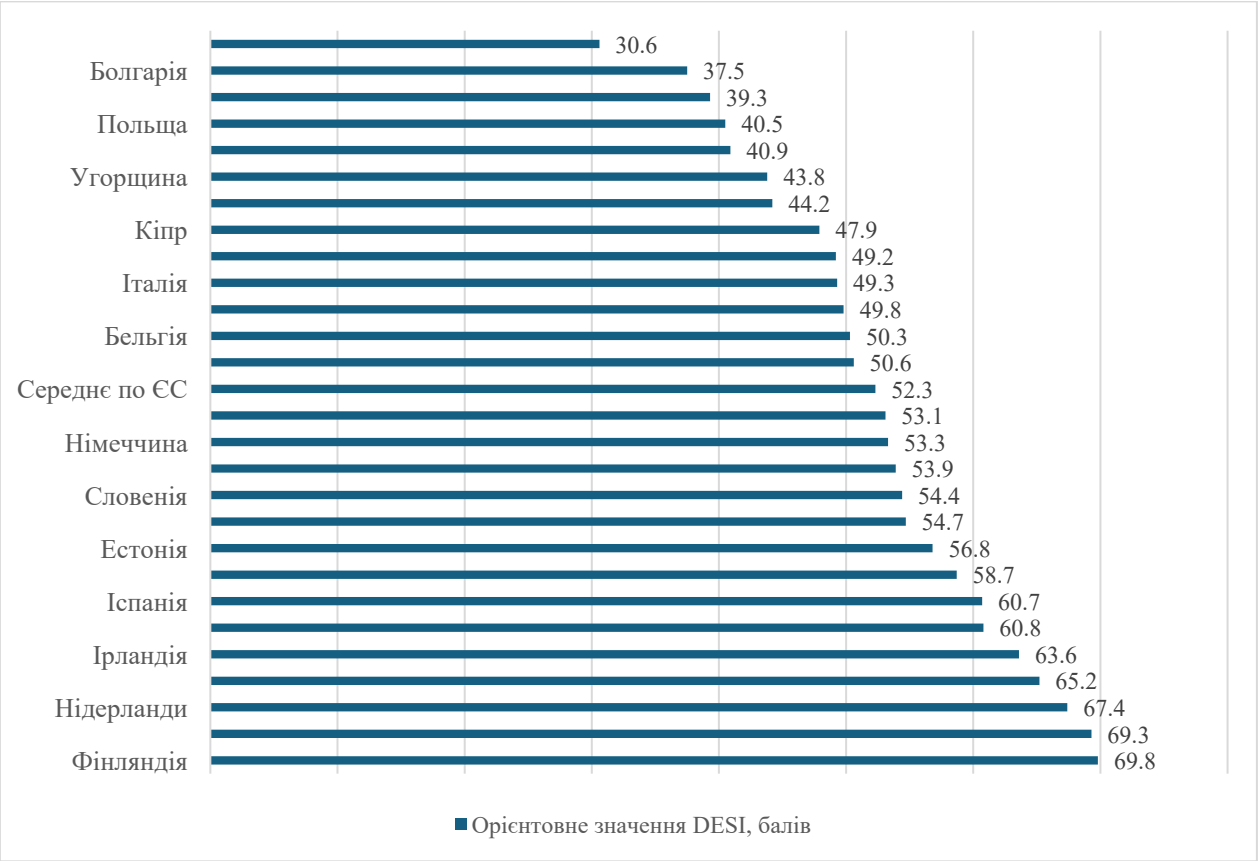


Рис. 3.11. Індекс цифрової економіки та суспільства (DESI) у країнах ЄС, 2022 р. [264]

Як свідчать дані рис. 3.11, у 2022 році лідерами за рівнем цифрового розвитку стали Фінляндія (69,8 бала), Данія (69,3 бала), Нідерланди (67,4 бала), Швеція (65,2 бала) та Ірландія (63,6 бала). Дані країни характеризуються високим рівнем цифрових компетентностей населення, широким доступом до швидкісного інтернету, активним впровадженням цифрових технологій у діяльність організацій та високою якістю електронних державних послуг. Саме ці держави першими реалізували масштабні проєкти цифрової трансформації охорони здоров'я, включаючи електронні медичні записи, електронні рецепти та телемедичні сервіси.

Середній показник по Європейському Союзу становив 52,3 бала, що свідчить про достатньо високий рівень цифровізації більшості держав-членів. До групи країн, які перевищують середньоєвропейський рівень, також належать Мальта, Іспанія, Люксембург, Естонія, Австрія, Словенія, Франція, Німеччина та Литва.

Аналіз структури Індексу цифрової економіки та суспільства показує, що найбільший внесок у загальний результат більшості країн забезпечують показники людського капіталу та цифрових державних послуг. Це свідчить про значну увагу європейських держав до розвитку цифрових навичок населення та створення електронних сервісів для громадян. Проте у багатьох країнах відносно нижчими залишаються показники інтеграції цифрових технологій у діяльність підприємств та організацій, що вказує на наявність потенціалу для подальшої цифрової трансформації.

Найнижчі значення Індексу цифрової економіки та суспільства зафіксовано в Румунії (30,6 бала), Болгарії (37,5 бала), Греції (39,3 бала), Польщі (40,5 бала) та Словаччині (40,9 бала). Незважаючи на певний прогрес у розвитку цифрової інфраструктури та державних сервісів, зазначені країни все ще відстають від середньоєвропейських показників за рівнем цифрових навичок населення та масштабами використання цифрових технологій.

Високий рівень цифрового розвитку європейських країн створює необхідні передумови для впровадження цифрових технологій у сфері охорони здоров'я. Одним із ключових індикаторів практичної реалізації цифрової трансформації медичної галузі є рівень розвитку електронних медичних записів (Electronic Health Records), які забезпечують накопичення, зберігання та обмін медичною інформацією між усіма учасниками системи охорони здоров'я. У зв'язку з цим доцільно проаналізувати рівень зрілості систем Electronic Health Records (Електронні медичні записи) у країнах Європи (рис. 3.12).

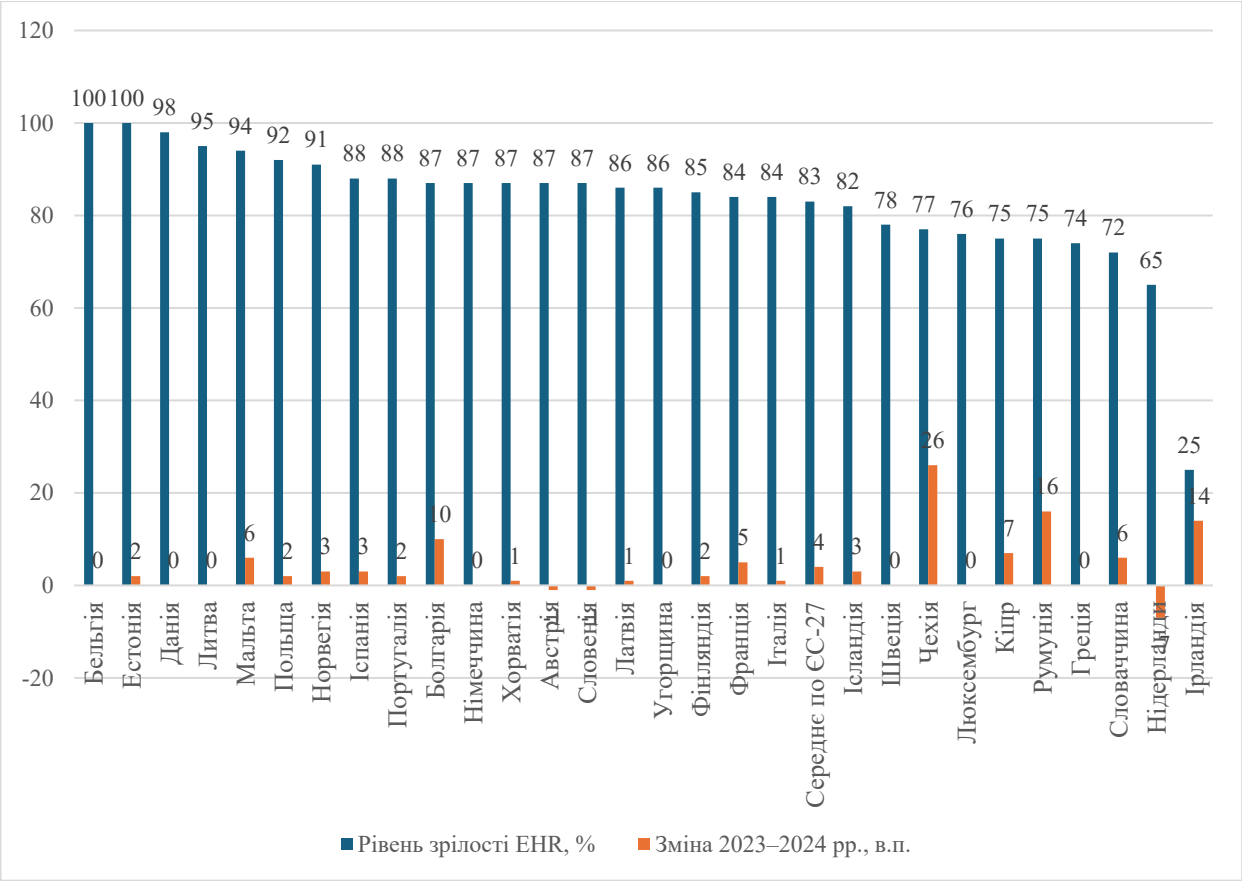


Рис. 3.12. Рівень зрілості доступу до електронних медичних записів (EHR) у країнах Європейського Союзу у 2024 році, % [81]

Середній показник зрілості EHR у країнах Європейського Союзу у 2024 році становив 83 %, що на 4 відсоткові пункти більше порівняно з попереднім роком. Це свідчить про поступове наближення держав-членів до стратегічної цілі ЄС щодо забезпечення повного доступу громадян до власних електронних медичних даних до 2030 року.

Абсолютними лідерами є Бельгія та Естонія, які досягли максимального рівня зрілості EHR – 100 %. Високі показники також демонструють Данія (98 %), Литва (95 %), Мальта (94 %) та Польща (92 %). Для цих країн характерним є комплексний розвиток цифрової інфраструктури охорони здоров'я, широке використання електронних медичних записів, електронних рецептів та цифрових сервісів для пацієнтів.

До групи країн із високим рівнем цифрової зрілості (понад 85 %) належать також Норвегія, Іспанія, Португалія, Болгарія, Німеччина, Хорватія, Австрія, Словенія, Латвія та Угорщина. Це свідчить про те, що більшість держав Європи вже сформували необхідну цифрову основу для подальшого розвитку телемедицини, систем підтримки клінічних рішень та технологій штучного інтелекту.

Водночас окремі країни демонструють нижчі показники цифрової зрілості. Зокрема, рівень розвитку EHR у Нідерландах становить 65 %, у Словаччині – 72 %, Греції – 74 %, Румунії та Кіпрі – по 75 %. Найнижчий показник зафіксовано в Ірландії – 25 %, що істотно відрізняє її від більшості інших країн Європейського Союзу.

Найбільший прогрес динаміки розвитку систем EHR у 2024 році продемонструвала Чехія (+26 в.п.), а також Румунія (+16 в.п.), Ірландія (+14 в.п.) та Болгарія (+10 в.п.). Це свідчить про активізацію процесів цифрової трансформації охорони здоров'я навіть у тих країнах, які раніше відставали за рівнем цифрового розвитку. Натомість негативна динаміка спостерігається в Нідерландах (-7 в.п.), Австрії (-1 в.п.) та Словенії (-1 в.п.), що може бути пов'язано зі зміною методики оцінювання або особливостями модернізації національних цифрових систем.

Оцінка рівня зрілості EHR дозволяє визначити ступінь розвитку електронних медичних записів у різних країнах Європи. Разом із тим важливим є дослідження не лише загального рівня їх впровадження, а й структури медичних даних, доступних через такі системи. Тому доцільно проаналізувати рівень доступності основних категорій медичної інформації в електронних медичних записах країн Європейського Союзу (рис. 3.13).

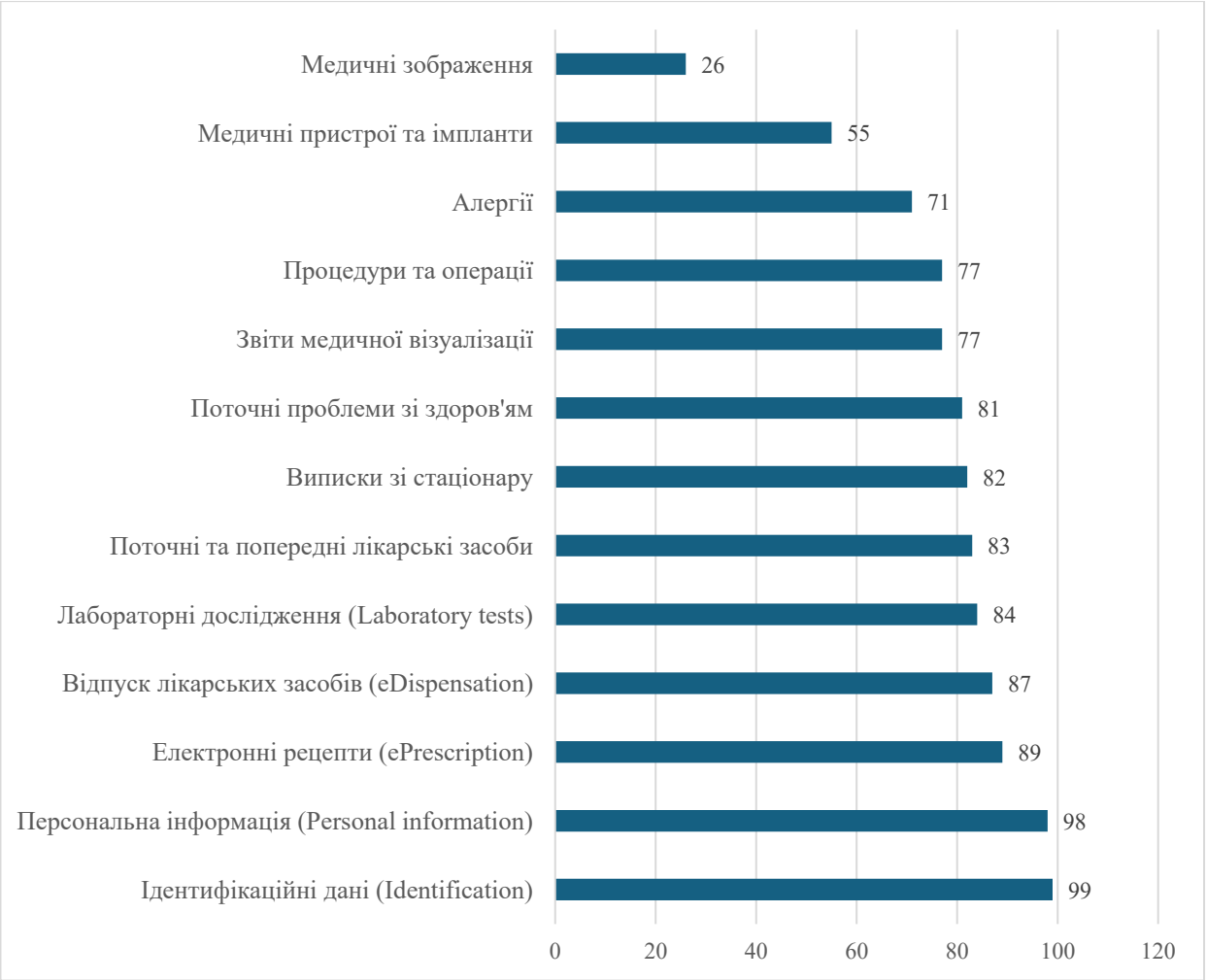


Рис. 3.13. Рівень зрілості доступності різних категорій медичних даних у системах EHR країн Європейського Союзу у 2024 році, %[]

Найвищий рівень зрілості характерний для базових категорій інформації, зокрема ідентифікаційних даних пацієнтів (99 %) та персональної інформації (98 %), що підтверджує майже повне охоплення населення цифровими медичними сервісами та високий рівень інтеграції електронних медичних записів у національні системи охорони здоров'я.

Особливо важливим є високий рівень доступності електронних рецептів (89 %) та інформації про відпуск лікарських засобів (87 %). Це свідчить про успішне впровадження цифрових механізмів фармацевтичного забезпечення населення та розвиток транскордонних електронних медичних послуг у межах Європейського Союзу. Високі показники також демонструють результати

лабораторних досліджень (84 %), відомості про поточні та попередні лікарські засоби (83 %), виписки зі стаціонару (82 %) та інформацію про поточні проблеми зі здоров'ям пацієнтів (81 %), що забезпечує комплексне інформаційне супроводження процесу надання медичної допомоги.

Середній рівень доступності характерний для таких категорій даних, як алергії (71 %), процедури та операції (77 %) та звіти медичної візуалізації (77 %). Це свідчить про поступове розширення функціональних можливостей електронних медичних записів та інтеграцію більш складних видів медичної інформації до цифрових систем охорони здоров'я.

Найнижчі показники зафіксовані щодо медичних пристроїв та імплантів (55 %) і особливо медичних зображень (26 %). Така ситуація пояснюється складністю стандартизації та передачі великих обсягів візуальних медичних даних, необхідністю використання спеціалізованих форматів зберігання інформації та забезпеченням високого рівня інтероперабельності між медичними інформаційними системами різних закладів охорони здоров'я.

Високий рівень цифрової зрілості електронних медичних записів та доступності медичних даних створює основу для формування єдиного європейського простору медичних даних. Саме тому одним із пріоритетних напрямів цифрової трансформації охорони здоров'я в Європейському Союзі стало створення European Health Data Space (EHDS), покликаного забезпечити безпечний транскордонний обмін медичною інформацією та підвищити ефективність використання даних у сфері охорони здоров'я.

5 березня 2025 року Регламент про Європейський простір даних охорони здоров'я був офіційно опублікований в Офіційному журналі Європейського Союзу та набрав чинності 26 березня 2025 року, започаткувавши перехідний етап його практичної реалізації. Запровадження European Health Data Space є одним із ключових напрямів побудови Європейського союзу охорони здоров'я та формування єдиного цифрового простору медичних даних.

Основною метою European Health Data Space є забезпечення громадянам держав-членів повного доступу до власних електронних медичних даних і можливості контролю над їх використанням, а також створення умов для безпечного транскордонного обміну медичною інформацією. Водночас регламент передбачає використання електронних даних про здоров'я для наукових досліджень, інноваційної діяльності, формування політики у сфері охорони здоров'я, забезпечення готовності до надзвичайних ситуацій та реагування на майбутні епідемічні загрози. Особливе значення EHDS має для розвитку персоналізованої медицини, підвищення безпеки пацієнтів, удосконалення офіційної медичної статистики та підтримки регуляторної діяльності.

Важливою складовою реалізації EHDS є гармонізація правових, організаційних та технічних вимог до систем електронних медичних записів (EHR), що сприятиме підвищенню їхньої інтероперабельності та сумісності в межах Європейського Союзу. Реалізація регламенту передбачає поетапне впровадження механізмів транскордонного обміну медичними даними, оскільки до 2029 року планується забезпечити обмін резюме пацієнтів та електронними рецептами, а до 2031 року – медичними зображеннями, результатами лабораторних досліджень та лікарняними виписками.

Таким чином, створення Європейського простору даних охорони здоров'я є свідченням переходу європейської системи охорони здоров'я від цифровізації окремих медичних сервісів до формування єдиної інтегрованої цифрової екосистеми управління медичними даними. Це створює необхідні передумови для подальшого розвитку телемедицини, технологій штучного інтелекту, персоналізованої медицини та інших інноваційних напрямів цифрової охорони здоров'я.

Важливим напрямом розвитку цифрової охорони здоров'я в Європейському Союзі є створення механізмів транскордонного обміну медичною інформацією між державами-членами. Реалізація цього завдання здійснюється через цифрову платформу MyHealth@EU, яка забезпечує взаємодію національних систем охорони здоров'я та створює умови для безперервного медичного супроводу громадян під час перебування за межами країни проживання.

Функціонування зазначеної системи спрямоване на забезпечення доступності ключових медичних даних незалежно від місця надання медичної допомоги. Насамперед це стосується електронних рецептів та узагальненої медичної інформації про пацієнта, що дозволяє лікарям отримувати необхідні відомості для прийняття клінічних рішень навіть у разі звернення пацієнта до закладу охорони здоров'я іншої країни. Такий підхід сприяє підвищенню якості медичної допомоги, мінімізації ризиків, пов'язаних із відсутністю інформації про стан здоров'я пацієнта, а також забезпечує безперервність лікування.

Особливе значення має можливість використання електронних рецептів у міжнародному форматі, що дозволяє пацієнтам отримувати необхідні лікарські засоби в інших країнах Європейського Союзу без повторного оформлення медичних документів. Одночасно система забезпечує доступ медичних працівників до найважливішої клінічної інформації, зокрема даних про алергічні реакції, попередні захворювання, призначене лікування та проведені медичні втручання.

Подальший розвиток транскордонних цифрових медичних сервісів передбачає поступове розширення переліку доступних даних шляхом інтеграції результатів лабораторних досліджень, медичних зображень, лікарняних виписок та інших складових електронної медичної документації. Це свідчить про перехід європейських країн до формування

єдиного цифрового медичного середовища, у межах якого медична інформація розглядається як стратегічний ресурс для підвищення ефективності, доступності та якості медичної допомоги [6].

Формування єдиного цифрового середовища охорони здоров'я та забезпечення доступності медичних даних створюють необхідні умови для розвитку цифрових медичних послуг. Одним із найбільш динамічних напрямів цифровізації є телемедицина, яка дозволяє надавати медичну допомогу дистанційно та підвищувати доступність медичних послуг для населення. У зв'язку з цим доцільно проаналізувати рівень розвитку телемедичних сервісів у країнах Європи (рис. 3.14).

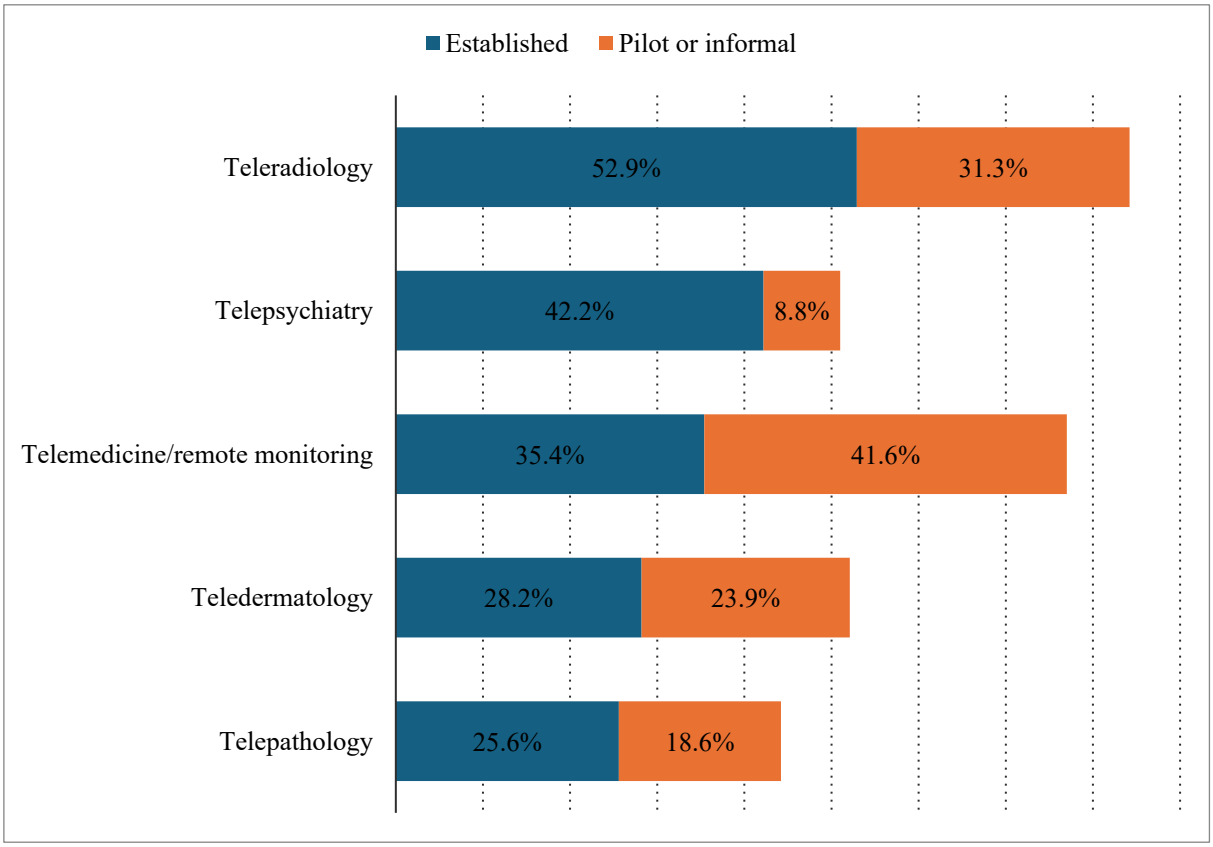


Рис. 3.14. Рівень зрілості телемедичних сервісів у країнах Європи у 2022 році [211]

[6] Electronic cross-border health services. Public Health. URL: https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/electronic-cross-border-health-services_en (date of access: 08.06.2026).

У результаті аналізу виявлено, що найбільш розвиненим напрямом телемедицини є телерадіологія, яка характеризується найвищим рівнем впровадження серед усіх досліджуваних сервісів. У 52,9 % країн телерадіологічні сервіси функціонують на постійній основі, тоді як ще у 31,3 % країн вони перебувають на етапі пілотного або часткового впровадження. Це пояснюється високою потребою в дистанційній інтерпретації результатів медичної візуалізації та можливістю ефективного використання кадрового потенціалу незалежно від місця розташування фахівців.

Другу позицію займає телепсихіатрія, яка впроваджена на постійній основі у 42,2 % країн. Поширення цього напряму значною мірою обумовлене зростанням потреби у забезпеченні доступності психіатричної допомоги та можливістю проведення консультацій без фізичної присутності пацієнта. Водночас лише 8,8 % країн використовують телепсихіатрію в межах пілотних проєктів, що свідчить про достатньо високий рівень її інституціоналізації.

Важливим напрямом цифровізації охорони здоров'я є телемедицина та дистанційний моніторинг пацієнтів, які функціонують у 35,4 % країн, тоді як ще у 41,6 % держав перебувають на стадії пілотного впровадження. Сукупний показник перевищує 77 %, що свідчить про високий потенціал розвитку технологій віддаленого спостереження за станом здоров'я пацієнтів та поступовий перехід до моделей безперервного медичного супроводу.

Менш поширеними залишаються теледерматологія та телепатологія. Частка країн, де теледерматологія впроваджена на постійній основі, становить 28,2 %, тоді як ще 23,9 % перебувають на етапі пілотного використання. Для телепатології відповідні показники складають 25,6 % та 18,6 %. Нижчий рівень поширення цих сервісів може бути пов'язаний із

необхідністю використання спеціалізованого обладнання, стандартизованих цифрових форматів медичних зображень та високих вимог до якості передачі даних.

Подальший розвиток телемедицини нерозривно пов'язаний із впровадженням сучасних цифрових технологій, які забезпечують автоматизацію медичних процесів, дистанційний моніторинг пацієнтів та підтримку прийняття клінічних рішень. Тому важливо дослідити готовність європейських країн до використання передових цифрових технологій у сфері охорони здоров'я (рис. 3.15).

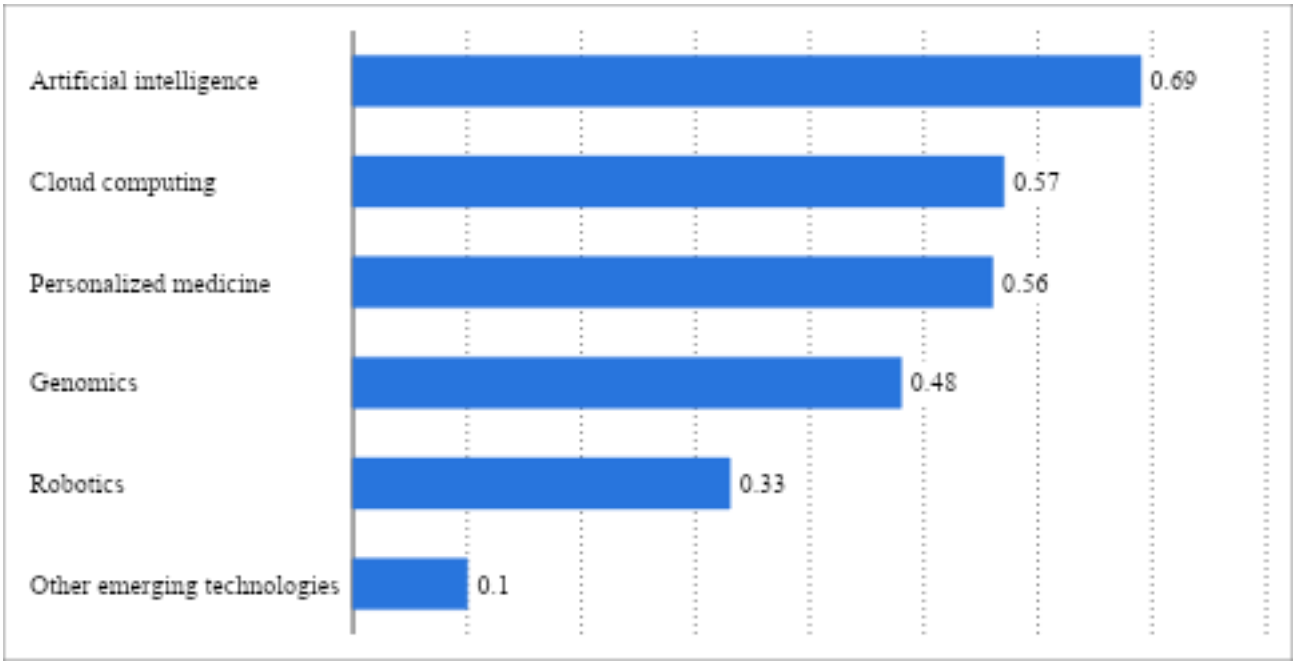


Рис. 3.15. Готовність країн Європи до впровадження передових цифрових технологій у сфері охорони здоров'я [7]

Отримані результати свідчать, що найбільшу увагу держави приділяють розвитку технологій штучного інтелекту, хмарних обчислень та персоналізованої медицини, які розглядаються як ключові інструменти підвищення ефективності медичних послуг та якості медичної допомоги.

[7] Ability to facilitate health technologies in Europe 2022| Statista. Statista. URL: https://www.statista.com/statistics/1421889/ability-to-facilitate-health-technologies-in-europe/ (date of access: 08.06.2026).

Найвищий показник готовності зафіксовано щодо технологій штучного інтелекту (69 %). Це свідчить про те, що більшість європейських країн розглядають штучний інтелект як один із пріоритетних напрямів цифрової трансформації охорони здоров'я. Використання алгоритмів штучного інтелекту відкриває можливості для автоматизації адміністративних процесів, підтримки клінічних рішень, прогнозування ризиків захворювань, аналізу великих масивів медичних даних та підвищення точності діагностики.

Високий рівень готовності також демонструють хмарні технології (57 %) та персоналізована медицина (56 %). Активне впровадження хмарних рішень забезпечує безпечне зберігання та обробку великих обсягів медичної інформації, підтримує функціонування електронних медичних записів і сприяє розвитку транскордонного обміну даними. Водночас персоналізована медицина дозволяє адаптувати профілактичні, діагностичні та лікувальні заходи до індивідуальних особливостей пацієнта, що відповідає сучасним тенденціям пацієнтоорієнтованого підходу в охороні здоров'я.

Важливе місце серед перспективних напрямів цифровізації займають геномні технології (48 %), які поступово інтегруються в клінічну практику та створюють передумови для розвитку прецизійної медицини. Разом із тим рівень готовності до впровадження робототехніки (33 %) залишається помірним, що може пояснюватися високою вартістю відповідного обладнання, складністю інтеграції роботизованих систем у медичні процеси та необхідністю значних інвестицій у розвиток інфраструктури.

Найнижчий показник характерний для категорії інших новітніх цифрових технологій (10 %), що свідчить про початковий етап їх поширення та відсутність достатнього практичного досвіду використання в більшості країн Європи.

Успішне впровадження інноваційних цифрових технологій у сфері охорони здоров'я залежить не лише від рівня технологічного розвитку, а й від готовності громадян використовувати цифрові сервіси та надавати доступ до власних медичних даних. У зв'язку з цим доцільно проаналізувати рівень готовності пацієнтів до цифрового обміну медичною інформацією (рис. 3.16).

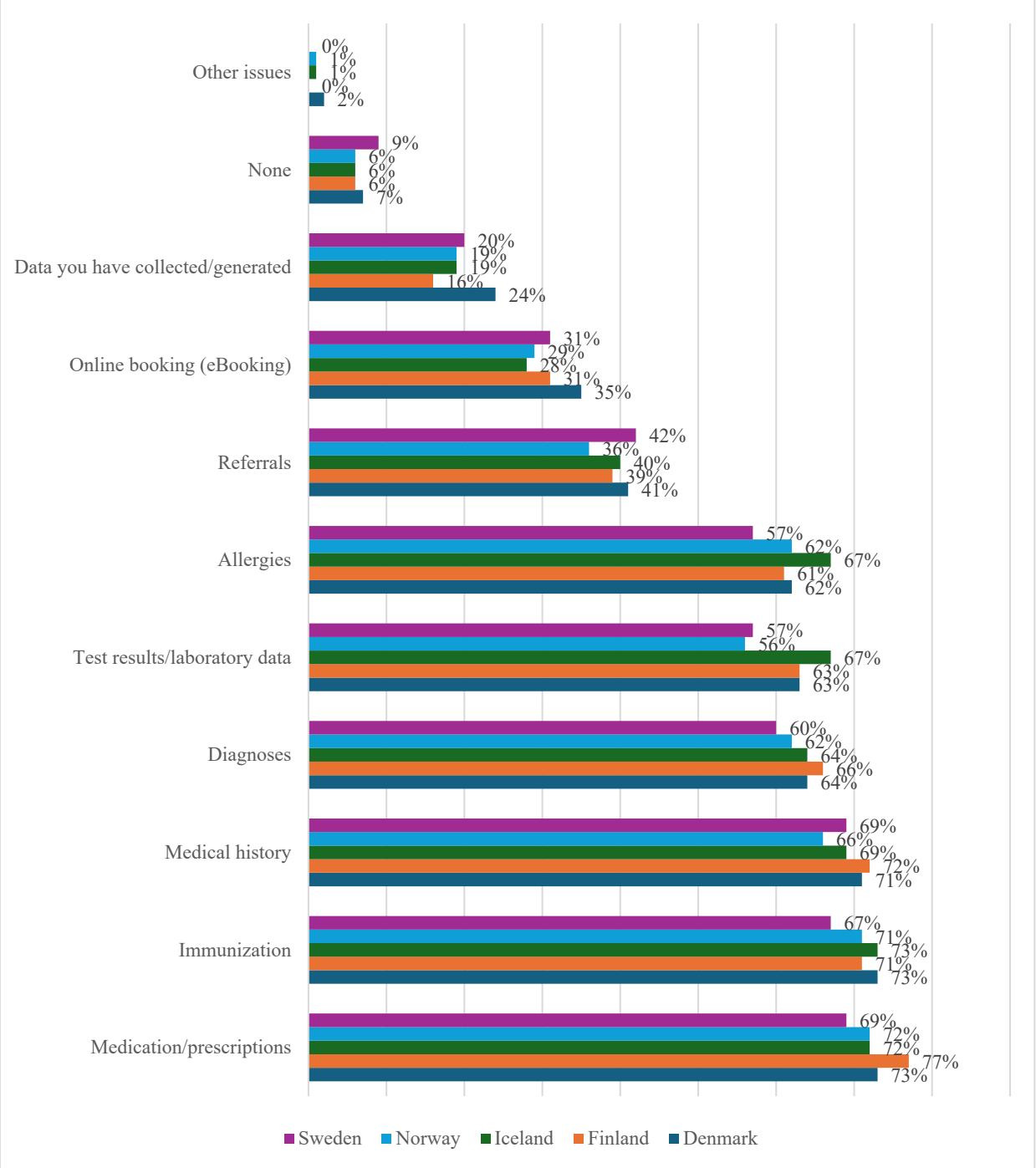


Рис. 3.16. Готовність пацієнтів до обміну медичними даними [221]

Аналіз отриманих результатів рис. 3.16 свідчить про високий рівень довіри населення до цифрових медичних сервісів та готовність громадян використовувати електронні інструменти управління власним здоров'ям.

Найвищий рівень готовності спостерігається щодо обміну інформацією про призначені лікарські засоби та рецепти, де показники в усіх досліджуваних країнах перевищують 70 %. Аналогічно високими є значення для даних про імунізацію, медичну історію, діагнози, а також результати лабораторних досліджень, що свідчить про усвідомлення пацієнтами важливості доступності повної медичної інформації для забезпечення безперервності лікування та підвищення якості медичної допомоги.

Достатньо високий рівень готовності також характерний для обміну інформацією про алергічні реакції, що має особливе значення для безпеки пацієнтів під час надання медичної допомоги. Разом з тим дещо нижчі показники спостерігаються щодо передачі направлень до лікарів, а також використання сервісів онлайн-запису на прийом (eBooking), хоча і в цих категоріях рівень готовності залишається відносно високим.

Найнижчі показники зафіксовані щодо обміну даними, які пацієнти самостійно збирають або генерують, а також щодо інших видів медичної інформації. Це може бути пов'язано з відсутністю єдиних стандартів інтеграції таких даних до електронних медичних записів, недостатньою поширеністю цифрових пристроїв моніторингу здоров'я або занепокоєнням щодо конфіденційності персональної інформації.

Високий рівень готовності пацієнтів до обміну медичними даними створює передумови для активного використання цифрових платформ охорони здоров'я. Саме цифрові портали забезпечують доступ громадян до медичної інформації та електронних сервісів, тому важливо оцінити напрями їх практичного використання в європейських країнах (рис. 3.17).

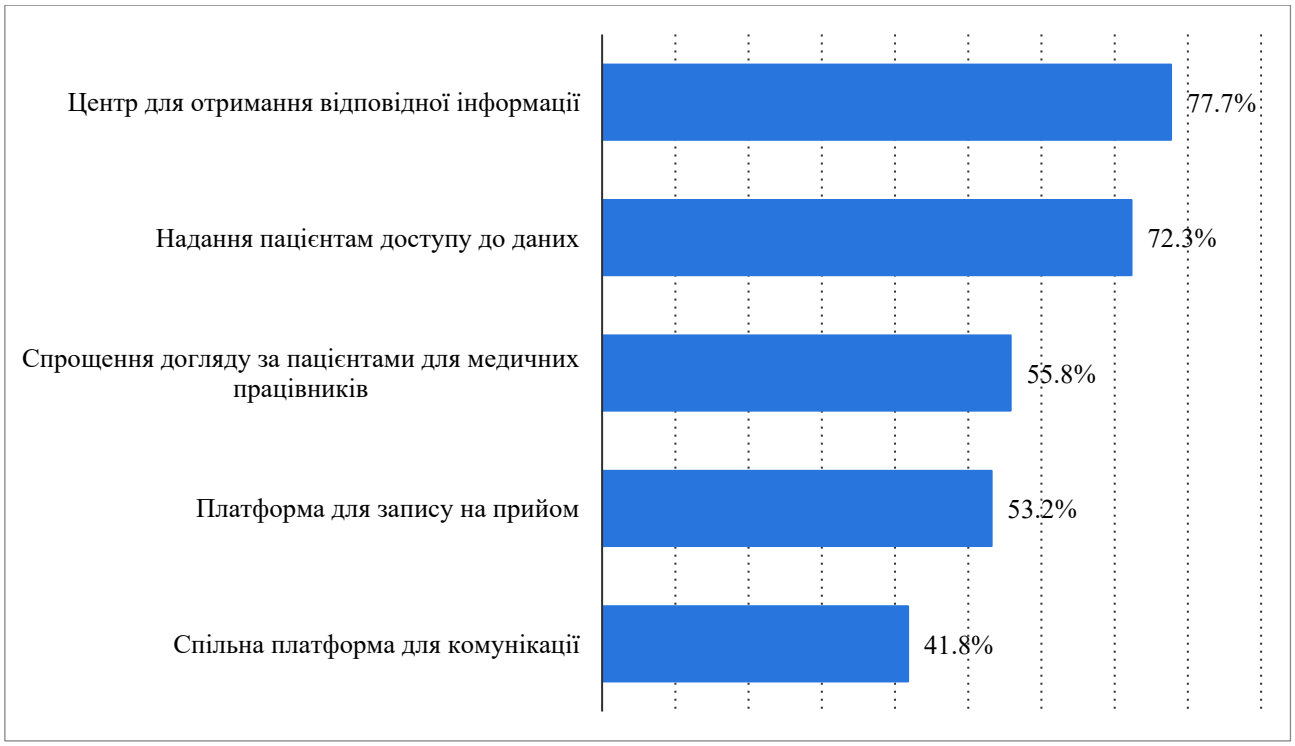


Рис. 3.17. Використання національних цифрових порталів охорони здоров'я в Європі [211]

З проведеного аналізу даних рис. 3.17 встановлено, що цифрові портали поступово перетворюються на ключовий інструмент організації медичних послуг та управління медичними даними. Найбільш поширеною функцією цифрових порталів є використання їх як центру отримання довідкової інформації, що характерно для 77,7 % досліджуваних систем. Це свідчить про значну роль електронних платформ у поширенні інформації про медичні послуги, профілактичні заходи, маршрути пацієнтів та порядок отримання медичної допомоги. Завдяки цьому громадяни отримують швидкий доступ до актуальної інформації без необхідності особистого звернення до медичних установ.

Другим за поширеністю напрямом є надання пацієнтам доступу до власних медичних даних, який реалізований у 72,3 % випадків. Такий показник підтверджує активний розвиток пацієнтоорієнтованого підходу в європейській системі охорони здоров'я та прагнення забезпечити

громадянам можливість контролювати власну медичну інформацію, переглядати результати обстежень, рецепти, медичні записи та інші відомості через електронні сервіси.

Важливим напрямом функціонування цифрових порталів є спрощення догляду за пацієнтами для медичних працівників, що характерно для 55,8 % систем. Це свідчить про поступове впровадження цифрових інструментів координації медичної допомоги, автоматизації документообігу та оптимізації процесів взаємодії між різними учасниками системи охорони здоров'я.

Понад половина досліджуваних порталів (53,2 %) використовуються як платформи для електронного запису на прийом до лікаря, що підтверджує зростання популярності електронних сервісів організації медичної допомоги. Використання таких інструментів сприяє підвищенню доступності медичних послуг, скороченню часу очікування та зменшенню адміністративного навантаження на медичні установи.

Найменш поширеною функцією є створення спільних платформ для комунікації між пацієнтами та медичними працівниками, які використовуються у 41,8 % випадків. Незважаючи на відносно нижчий показник, цей напрям залишається перспективним у контексті розвитку телемедицини, дистанційного консультування та безперервного супроводу пацієнтів.

Розвиток цифрових порталів та електронних сервісів супроводжується активним впровадженням технологій штучного інтелекту, які відкривають нові можливості для автоматизації медичних процесів, підтримки клінічних рішень та підвищення ефективності управління системою охорони здоров'я. У зв'язку з цим доцільно проаналізувати основні напрями використання штучного інтелекту в охороні здоров'я європейських країн (рис. 3.18).

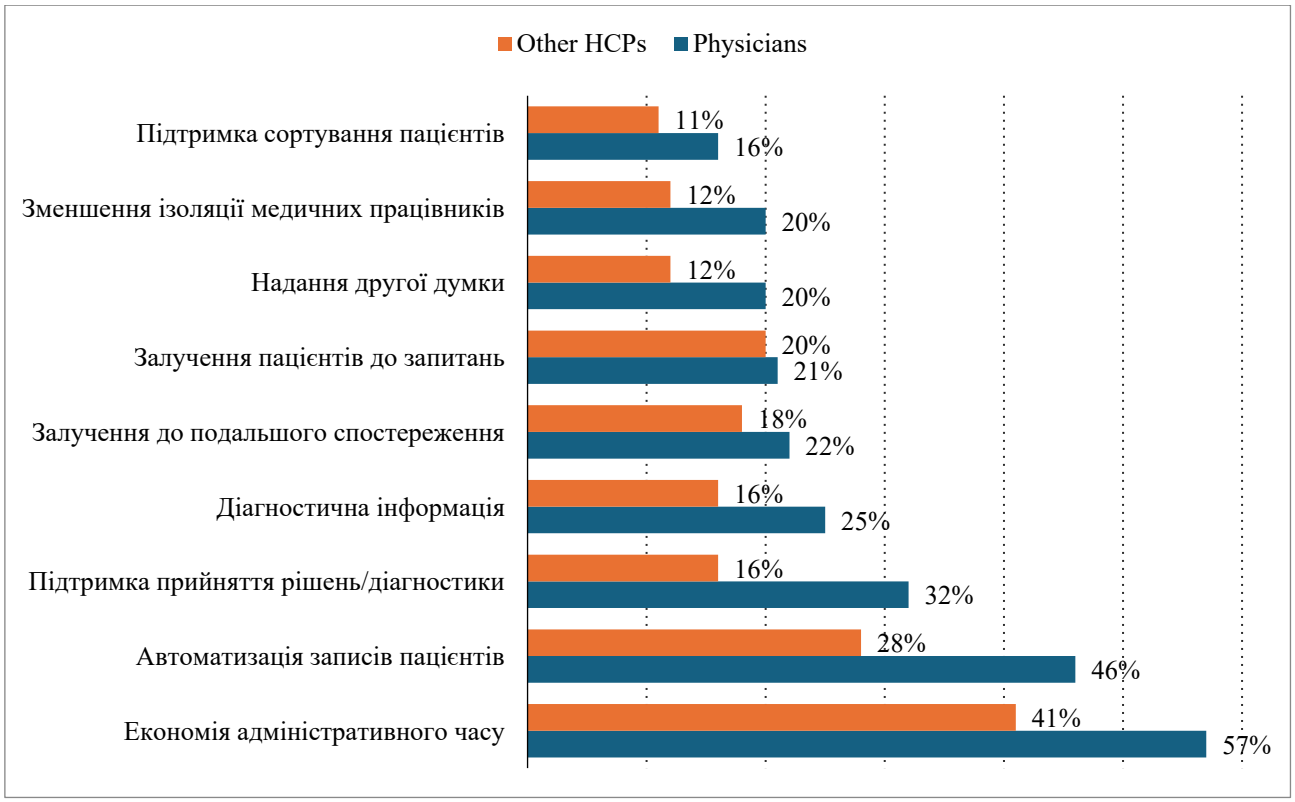


Рис. 3.18. Використання штучного інтелекту в системі охорони здоров'я європейських країн [92]

Найбільш значущою перевагою використання штучного інтелекту медичні працівники вважають економію адміністративного часу, що відзначили 57 % лікарів та 41 % інших працівників сфери охорони здоров'я. Це свідчить про високий потенціал AI щодо автоматизації документообігу, підготовки медичної документації, обробки даних пацієнтів та інших рутинних процесів, які займають значну частину робочого часу медичного персоналу.

Високі показники також характерні для напряму автоматизації записів пацієнтів, який підтримали 46 % лікарів та 28 % інших працівників. Отримані результати підтверджують, що автоматизовані системи обробки медичної інформації здатні підвищити точність ведення електронних медичних записів та знизити навантаження на персонал.

Важливим напрямом використання штучного інтелекту є підтримка прийняття клінічних рішень та діагностики, що відзначили 32 % лікарів та 16 % інших фахівців. Крім того, 25 % лікарів вказали на ефективність AI для отримання діагностичної інформації. Це свідчить про поступову інтеграцію інтелектуальних алгоритмів у клінічну практику та використання технологій машинного навчання для аналізу медичних даних і підтримки процесу встановлення діагнозу.

Серед інших переваг застосування штучного інтелекту респонденти відзначають залучення пацієнтів до процесу лікування (21 %), покращення подальшого спостереження за пацієнтами (18–19 %), надання другої експертної думки (20 % лікарів) та зменшення професійної ізоляції медичних працівників (20 % лікарів). Це свідчить про потенціал AI не лише як технології автоматизації, а й як інструменту підтримки комунікації та координації медичної допомоги.

Відносно нижчі показники спостерігаються щодо використання штучного інтелекту для сортування пацієнтів (тріажу), що може бути пов'язано з необхідністю забезпечення високої точності алгоритмів та збереженням ключової ролі медичного працівника у прийнятті остаточних клінічних рішень.

Поширення технологій штучного інтелекту та цифрових медичних сервісів потребує відповідного нормативно-правового та організаційного забезпечення. Тому важливим аспектом цифрової трансформації охорони здоров'я є інтеграція телемедицини до національних стратегій та політик розвитку охорони здоров'я, що зумовлює необхідність аналізу особливостей впровадження телемедичних технологій у європейських країнах (рис. 3.19).

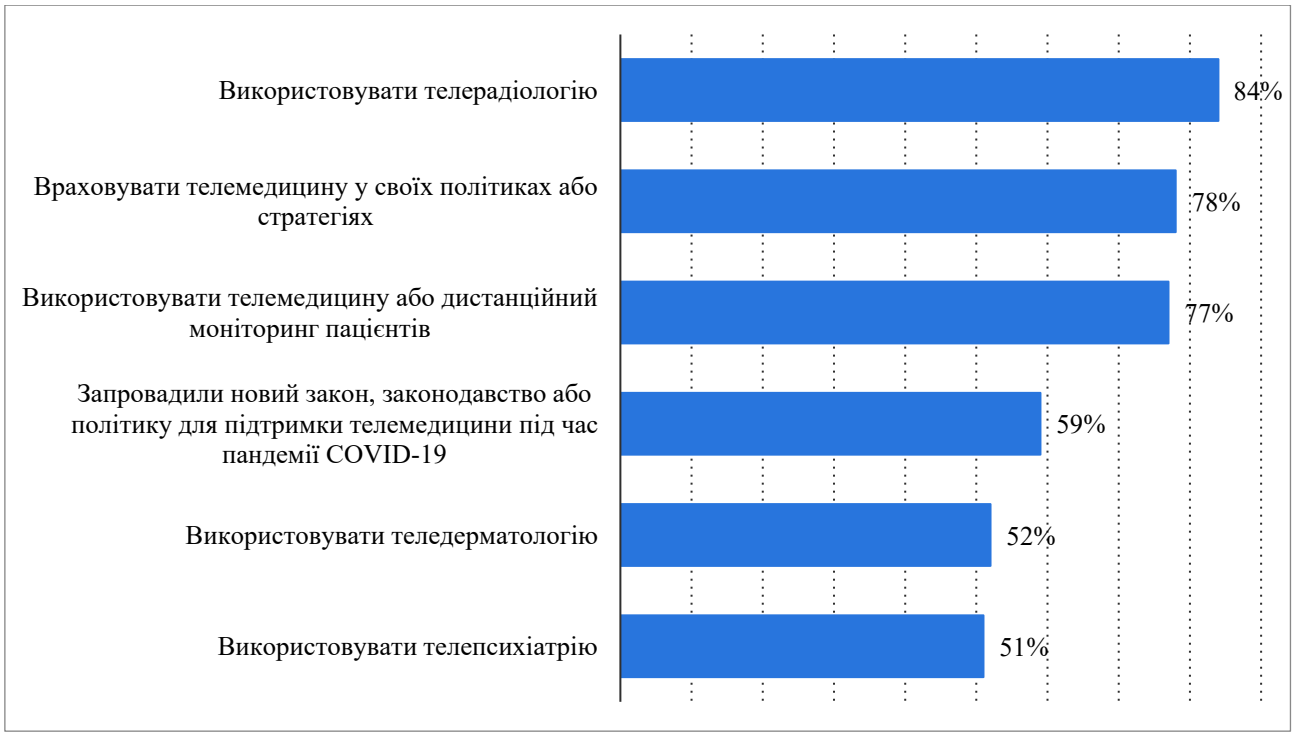


Рис. 3.19. Використання телемедичних технологій та політик у країнах Європи у 2022 році [261]

Найбільш поширеним напрямом є використання телерадіології, яке впроваджено у 84 % країн Європи. Такий високий показник пояснюється можливістю дистанційної передачі та інтерпретації результатів медичної візуалізації, що дозволяє ефективніше використовувати кадровий потенціал медичних установ та підвищувати оперативність діагностики. Телерадіологія стала одним із перших і найбільш успішних напрямів розвитку телемедичних послуг у європейських країнах.

Важливим результатом цифрової трансформації охорони здоров'я є те, що 78 % країн враховують телемедицину у своїх національних політиках або стратегіях розвитку охорони здоров'я. Це свідчить про перехід від окремих пілотних проєктів до системного впровадження телемедичних технологій на державному рівні та визнання їх важливим інструментом модернізації медичної сфери.

Високий рівень поширення також демонструють сервіси телемедицини та дистанційного моніторингу пацієнтів, які використовуються у 77 % досліджуваних країн. Активне впровадження таких технологій дозволяє здійснювати безперервне спостереження за станом здоров'я пацієнтів, своєчасно реагувати на зміни клінічних показників та забезпечувати медичний супровід без необхідності особистого відвідування закладів охорони здоров'я.

Особливу увагу привертає той факт, що 59 % країн запровадили нове законодавство або політики для підтримки телемедицини під час пандемії COVID-19. Це підтверджує, що пандемія стала потужним каталізатором цифрової трансформації медичних систем та прискорила розвиток дистанційних форм надання медичної допомоги.

Серед спеціалізованих напрямів телемедицини найбільшого поширення набули теледерматологія (52 %) та телепсихіатрія (51 %). Розвиток цих сервісів пов'язаний із можливістю проведення консультацій та спостереження за пацієнтами дистанційно без суттєвого зниження якості медичної допомоги. Особливо актуальним їх використання стало для забезпечення доступності спеціалізованої допомоги у віддалених регіонах та для осіб з обмеженою мобільністю.

Отже, проведене дослідження дозволило встановити, що європейські країни демонструють високий рівень розвитку цифрової охорони здоров’я та формують одну з найбільш розвинених цифрових медичних екосистем у світі. Аналіз індексу DESI засвідчив наявність суттєвих відмінностей між країнами Європи за рівнем цифрової готовності, водночас більшість держав-членів ЄС характеризуються високими показниками розвитку цифрової інфраструктури, цифрових навичок населення, інтеграції цифрових технологій та цифрових публічних послуг.

Встановлено, що ключовим елементом цифрової трансформації охорони здоров'я в Європейському Союзі є розвиток систем електронних медичних записів (EHR), середній рівень зрілості яких у країнах ЄС у 2024 році становив 83 %. Найвищий рівень цифрової зрілості EHR зафіксовано в Бельгії та Естонії, тоді як окремі країни продовжують перебувати на етапі активного розвитку цифрових медичних систем. Дослідження структури медичних даних показало, що найбільш доступними категоріями інформації є ідентифікаційні дані пацієнтів, персональна інформація, електронні рецепти та дані про відпуск лікарських засобів, що свідчить про високий рівень цифрової інтеграції базових медичних сервісів.

Важливим результатом цифрової трансформації стало формування Європейського простору даних охорони здоров'я (EHDS) та розвиток системи "MyHealth@EU", які створюють організаційні та технологічні передумови для транскордонного обміну медичними даними, забезпечення безперервності медичної допомоги та розширення доступу громадян до власної медичної інформації. Реалізація зазначених ініціатив свідчить про поступовий перехід від національних моделей цифровізації до формування єдиного цифрового медичного простору Європейського Союзу.

Слід відзначити, що одним із найбільш динамічних напрямів цифровізації охорони здоров'я є розвиток телемедичних сервісів. Найвищий рівень зрілості демонструють телерадіологія, дистанційний моніторинг пацієнтів та телепсихіатрія. Водночас у більшості європейських країн сформовано позитивне ставлення до подальшого розвитку телемедицини та її інтеграції до національної політики охорони здоров'я.

Під час проведеного аналізу стану цифровізації охорони здоров'я європейських країн встановлено, що перспективним напрямом цифрової трансформації є впровадження інноваційних цифрових технологій,

насамперед штучного інтелекту, хмарних обчислень, персоналізованої медицини, геноміки та роботизованих систем. При цьому використання технологій штучного інтелекту зосереджується переважно на автоматизації адміністративних процесів, підтримці клінічної діагностики та оптимізації роботи медичних працівників. Водночас успішність цифрової трансформації значною мірою залежить від готовності пацієнтів до використання цифрових сервісів та обміну медичними даними, що підтверджується високим рівнем підтримки цифрових медичних платформ у європейських країнах.

Таким чином, основними тенденціями цифровізації систем охорони здоров'я європейських країн є розвиток електронних медичних записів, формування єдиного простору медичних даних, розширення транскордонних цифрових сервісів, поширення телемедицини, інтеграція технологій штучного інтелекту та посилення ролі пацієнта в управлінні власними медичними даними. Сукупність зазначених процесів свідчить про перехід європейських систем охорони здоров'я до людиноцентричної цифрової моделі, заснованої на використанні даних, інтероперабельності інформаційних систем та інноваційних технологій.

3.3. Сучасний стан та основні напрями цифрової трансформації системи охорони здоров'я України

Упродовж останнього десятиліття в Україні відбувається активна цифрова трансформація системи охорони здоров'я, яка стала одним із ключових напрямів реформування медичної галузі. Запровадження електронної системи охорони здоров'я eHealth, розвиток цифрових сервісів Національної служби здоров'я України, впровадження електронних рецептів, електронних направлень, медичних інформаційних систем та інтеграція окремих медичних послуг із платформою «Дія» сприяли підвищенню прозорості управлінських процесів, доступності медичної допомоги та ефективності використання бюджетних коштів.

Особливої актуальності цифровізація охорони здоров'я набула в умовах воєнного стану, коли цифрові технології стали важливим інструментом забезпечення безперервності надання медичних послуг, збереження медичних даних пацієнтів та підтримки функціонування медичної системи в умовах значних безпекових викликів.

Після аналізу світового та європейського досвіду цифрової трансформації охорони здоров'я доцільним є дослідження особливостей розвитку цифрової системи охорони здоров'я України. В умовах реформування медичної галузі, європейської інтеграції та необхідності забезпечення безперервності медичних послуг в умовах воєнного стану цифровізація стала одним із ключових напрямів державної політики у сфері охорони здоров'я. Впровадження електронної системи охорони здоров'я, розвиток електронних медичних записів, електронних рецептів, електронних направлень, цифрових сервісів для пацієнтів та медичних працівників сприяли підвищенню доступності, прозорості та ефективності медичної допомоги.

З метою оцінювання результативності цифрової трансформації системи охорони здоров'я України у даному підрозділі доцільно:

– проаналізувати розвиток електронної системи охорони здоров'я України (ЕСОЗ);

– дослідити динаміку укладення декларацій між пацієнтами та лікарями первинної медичної допомоги;

– оцінити масштаби накопичення електронних медичних записів;

– проаналізувати динаміку використання електронних рецептів та електронних направлень;

– дослідити роль Національної служби здоров'я України у функціонуванні цифрової системи охорони здоров'я;

– охарактеризувати інтеграцію цифрових медичних сервісів із державними цифровими платформами;

– визначити основні результати та перспективи цифрової трансформації охорони здоров'я України.

Стратегічні орієнтири розвитку цифрової охорони здоров'я визначені Міністерством охорони здоров'я України у межах реалізації державної політики цифрової трансформації галузі, яка передбачає формування єдиного цифрового медичного простору, розвиток сервісів на основі медичних даних та інтеграцію національної системи охорони здоров'я до європейського цифрового середовища. Одним із ключових напрямів цифрової трансформації системи охорони здоров'я України стало впровадження електронної системи охорони здоров'я (ЕСОЗ), яка забезпечила цифровізацію взаємодії між пацієнтами, медичними працівниками, закладами охорони здоров'я та державними органами управління. Базовим елементом функціонування ЕСОЗ є система електронних декларацій про вибір лікаря первинної медичної допомоги, що дозволяє формувати електронний реєстр пацієнтів та забезпечує подальше використання цифрових медичних сервісів. Для оцінювання рівня охоплення населення цифровими медичними послугами проаналізуємо динаміку подання декларацій у розрізі вікових груп населення (рис. 3.20).

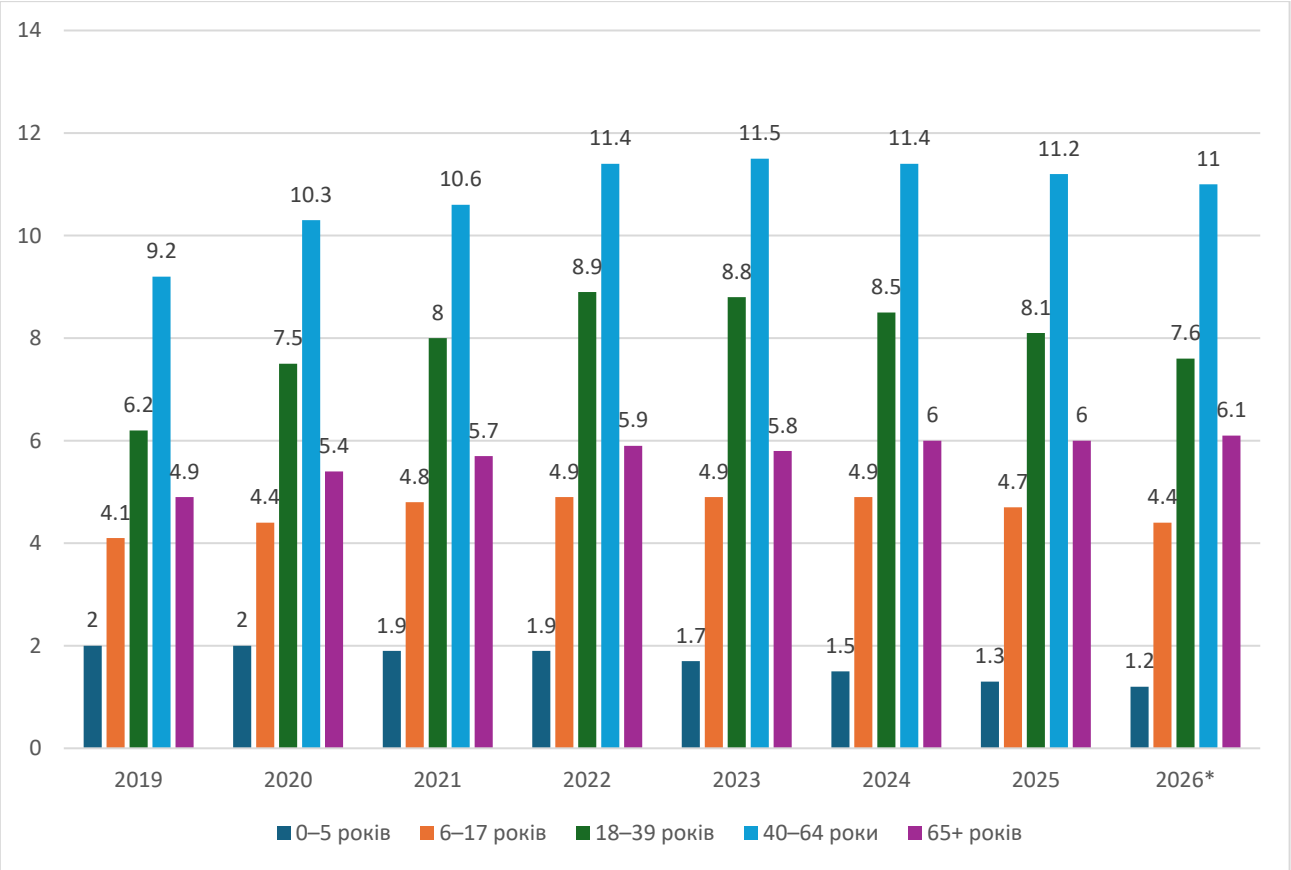


Рис. 3.20. Статистика поданих декларацій про вибір лікаря первинної медичної допомоги [68]

Проведений аналіз даних рис. 3.20 свідчить про стрімке поширення електронних декларацій після запуску медичної реформи та впровадження ЕСОЗ у 2018 році. Найбільш чисельною групою користувачів системи протягом усього періоду залишалися громадяни віком 40–64 роки. Кількість укладених декларацій у цій віковій категорії зросла з менш ніж 1 млн у 2018 році до 11,4 млн у 2024 році, після чого стабілізувалася на рівні близько 11,0 млн у 2026 році.

Другою за чисельністю групою стали особи віком 18–39 років. Кількість декларацій у цій категорії збільшилася до 8,9 млн у 2022 році, однак у подальшому спостерігається поступове скорочення показника до 7,6 млн осіб у 2026 році.

Серед населення віком понад 65 років кількість декларацій демонструвала стабільне зростання протягом усього досліджуваного періоду з близько 1 млн у 2018 році до понад 6 млн у 2026 році. Це свідчить про поступове залучення осіб старшого віку до використання цифрових інструментів охорони здоров'я.

Для вікової групи 6–17 років характерне зростання кількості декларацій до майже 5 млн у 2022–2023 роках із подальшим незначним зменшенням до 4,4 млн у 2026 році. Водночас у групі дітей віком 0–5 років після досягнення максимального значення близько 2 млн декларацій у 2019–2020 роках спостерігається поступове скорочення показника до 1,2 млн у 2026 році, що значною мірою пояснюється демографічними процесами та зменшенням чисельності дитячого населення.

На наступному рис. 3.21 відображено показники накопичення медичних електронних записів в електронній системі охорони здоров'я України за 2022–2025 рр.

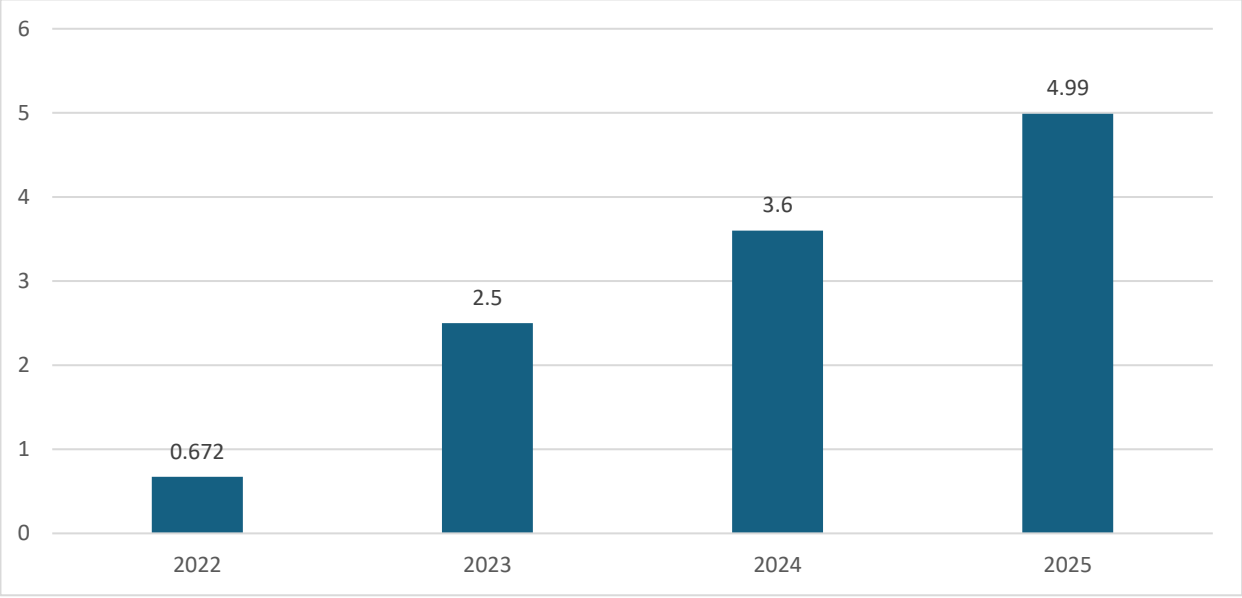


Рис. 3.21. Динаміка накопичення медичних електронних записів в електронній системі охорони здоров'я України у 2022–2025 рр., млрд [67]

Отже, аналіз даних рис. 3.21 свідчить про стрімке зростання кількості медичних електронних записів в електронній системі охорони здоров'я

України протягом 2022–2025 років. Якщо у 2022 році в системі було накопичено 672 млн електронних медичних записів, то вже у 2023 році їх кількість зросла до 2,5 млрд, тобто майже у 3,7 раза. У 2024 році обсяг накопичених даних досяг 3,6 млрд записів, а у 2025 році – майже 5 млрд записів.

Зростання кількості електронних записів майже до 5 млрд у 2025 році свідчить про масштабне впровадження електронного документообігу в медичній сфері, формування єдиного цифрового медичного простору та створення інформаційної основи для подальшого розвитку електронних рецептів, електронних направлень, телемедицини та аналітики медичних даних.

Одним із найбільш результативних напрямів цифрової трансформації системи охорони здоров'я України стало впровадження електронного рецепта, який забезпечив автоматизацію процесу призначення та відпуску лікарських засобів, підвищив прозорість обігу медикаментів і спростив доступ населення до фармацевтичних послуг. Особливого значення електронний рецепт набув після поширення його використання на програму «Доступні ліки», антибактеріальні препарати та наркотичні лікарські засоби. З метою оцінки динаміки використання електронного рецепта в Україні на рис. 3.22 представлено зміну кількості погашених рецептів упродовж 2019–2026 років.

Результати аналізу свідчать про стале поширення практики використання електронних рецептів в Україні. У 2019 році кількість погашених електронних рецептів становила 9,2 млн, а вже у 2020 році зросла до 11,8 млн, що відповідає приросту на 28,3 %. У 2021 році показник продовжив зростати та досяг 12,1 млн рецептів.

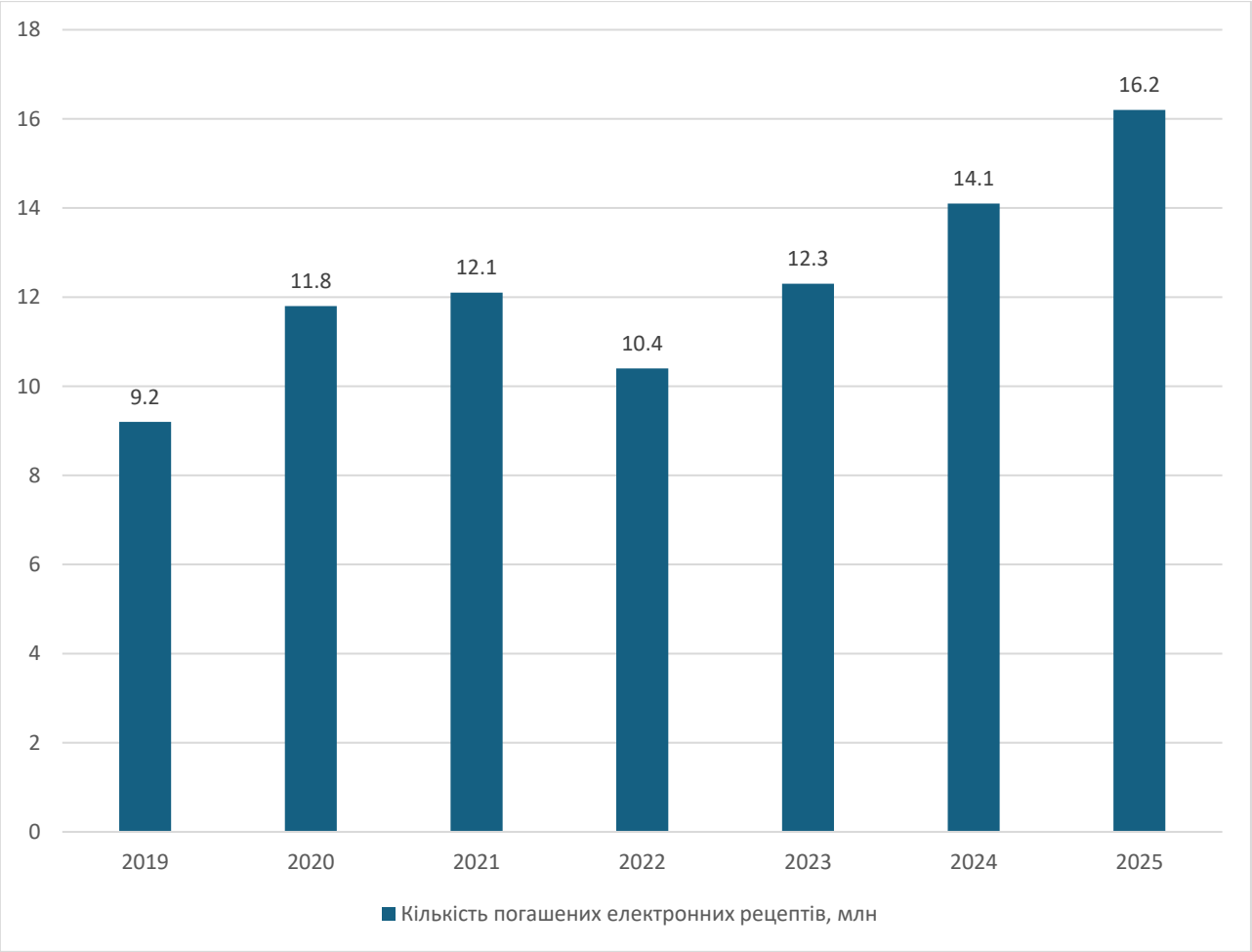


Рис. 3.22. Динаміка кількості погашених електронних рецептів в Україні у 2019–2026 рр. [16]

Певне зниження спостерігалося у 2022 році, коли кількість погашених електронних рецептів скоротилася до 10,4 млн. Таку динаміку можна пов'язати з негативним впливом повномасштабної війни на функціонування медичної інфраструктури та доступ населення до медичних послуг.

Починаючи з 2023 року, спостерігається відновлення позитивної тенденції. Кількість погашених електронних рецептів зросла до 12,3 млн у 2023 році та до 14,1 млн у 2024 році. Найвище значення за досліджуваний період було зафіксовано у 2025 році – 16,2 млн рецептів, що майже в 1,8 раза перевищує рівень 2019 року.

Таким чином, результати аналізу підтверджують високий рівень інтеграції електронного рецепта в систему охорони здоров'я України. Стійке зростання кількості погашених електронних рецептів демонструє підвищення рівня цифрової зрілості національної системи охорони здоров'я, розширення використання електронних медичних сервісів та зростання довіри населення до цифрових інструментів отримання медичної допомоги.

Наступним елементом цифрової трансформації системи охорони здоров'я України стало впровадження електронного направлення, яке забезпечило цифровізацію процесу скерування пацієнтів до спеціалізованих медичних закладів, діагностичних досліджень та консультацій лікарів. Використання електронних направлень сприяє підвищенню прозорості маршруту пацієнта, покращенню координації між рівнями медичної допомоги та формуванню єдиного інформаційного простору в системі охорони здоров'я. Для оцінювання масштабів використання даного інструменту проаналізуємо динаміку створених електронних направлень в Україні на рис. 3.23.

Дані рис. 3.23 свідчать про стрімке зростання кількості створених електронних направлень протягом досліджуваного періоду. У 2020 році було створено лише 20,1 млн електронних направлень, тоді як уже у 2021 році їх кількість збільшилася майже у чотири рази та досягла 79,3 млн. Подальше зростання спостерігалося у 2022 році, коли показник становив 130,8 млн направлень.

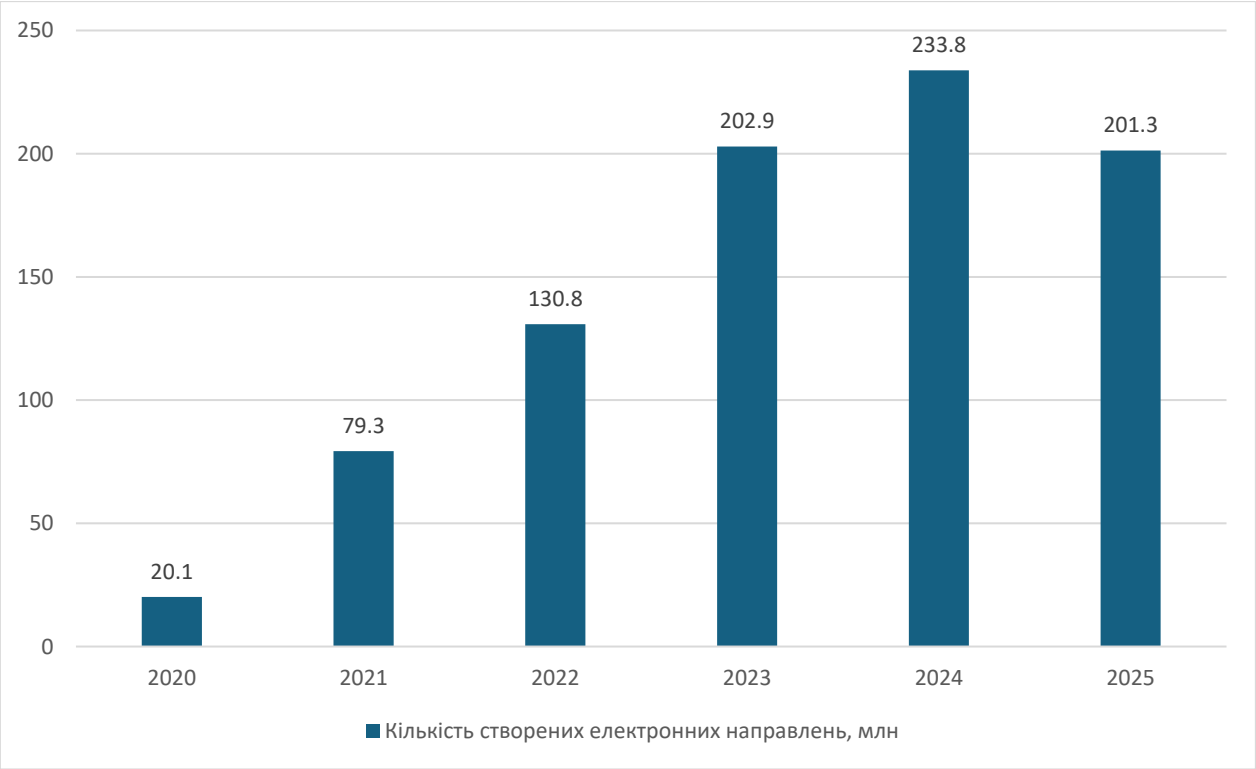


Рис. 3.23. Динаміка кількості створених електронних направлень в Україні у 2020–2026 рр., млн. [1]

Найбільш інтенсивне збільшення кількості електронних направлень відбулося у 2023 році, коли їх кількість зросла до 202,9 млн, а у 2024 році досягла максимального значення за досліджуваний період – 233,8 млн. Порівняно з 2020 роком обсяг створених електронних направлень збільшився більш ніж у 11 разів, що свідчить про високий рівень інтеграції цифрових сервісів у процес організації медичної допомоги.

У 2025 році кількість створених направлень дещо зменшилася до 201,3 млн, однак показник залишався суттєво вищим порівняно з попередніми роками. Значення 84,2 млн у 2026 році не відображає завершений річний цикл та характеризує лише поточний стан на момент формування звітності.

Вагомим індикатором ефективності функціонування електронного рецепта є співвідношення між кількістю виписаних та фактично погашених рецептів. Аналіз цього показника дозволяє оцінити рівень використання

цифрового сервісу пацієнтами, доступність лікарських засобів та результативність функціонування електронної системи охорони здоров'я. Для визначення тенденцій розвитку електронного рецепта в Україні проаналізуємо динаміку виписування та погашення рецептів протягом 2019–2024 років (рис. 3.24).

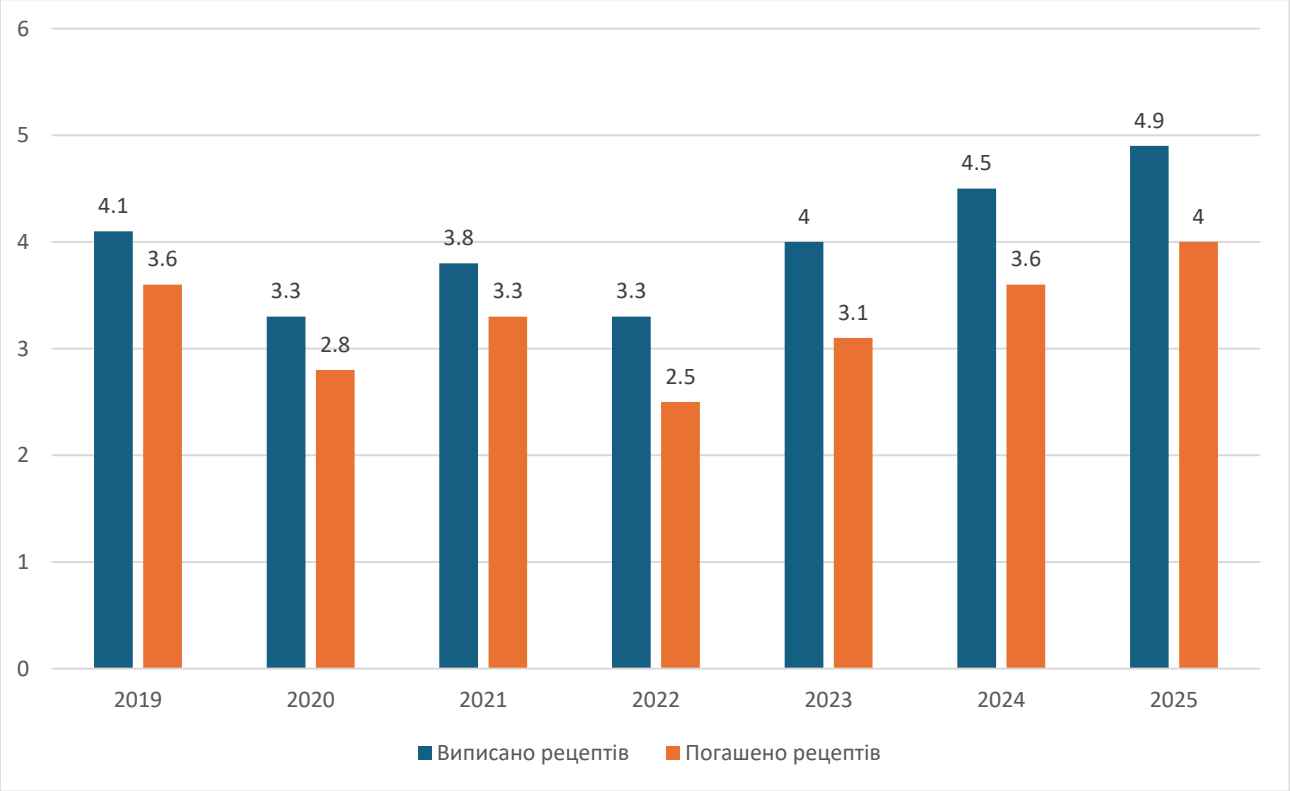


Рис. 3.24. Динаміка виписування та погашення електронних рецептів в Україні у 2019–2026 рр., млн. [15]

Отже, результати аналізу даних рис. 3.24 свідчать про стале зростання кількості як виписаних, так і погашених електронних рецептів протягом досліджуваного періоду. У 2019 році кількість виписаних рецептів становила 4,1 млн, а погашених – 3,6 млн. У 2020–2022 роках спостерігалися певні коливання показників, зокрема скорочення кількості погашених рецептів до 2,5 млн у 2022 році, що було зумовлено негативним впливом воєнних дій на функціонування медичної інфраструктури та доступність медичних послуг.

Починаючи з 2023 року, система демонструє стале відновлення та подальше зростання. Кількість виписаних рецептів збільшилася з 4,0 млн у 2023 році до 4,9 млн у 2025 році, тоді як кількість погашених рецептів зросла з 3,1 млн до 4,0 млн відповідно. У 2026 році показники досягли найвищих значень за весь досліджуваний період — 5,4 млн виписаних та 4,5 млн погашених рецептів.

Слід відзначити, що протягом усього періоду кількість погашених рецептів залишається дещо меншою за кількість виписаних, що є характерним для функціонування систем електронного рецепта та пояснюється тим, що частина призначень не реалізовується пацієнтами.

Визначною складовою функціонування електронної системи охорони здоров'я є забезпечення достовірності та актуальності даних пацієнтів шляхом їх верифікації через державні реєстри. Верифікація персональних даних дозволяє підвищити якість медичної інформації, запобігти дублюванню записів, забезпечити коректне надання медичних послуг та ефективне використання державних ресурсів. З метою оцінювання рівня достовірності даних в електронній системі охорони здоров'я проаналізуємо результати верифікації пацієнтів за основними державними реєстрами на рис. 3.25.

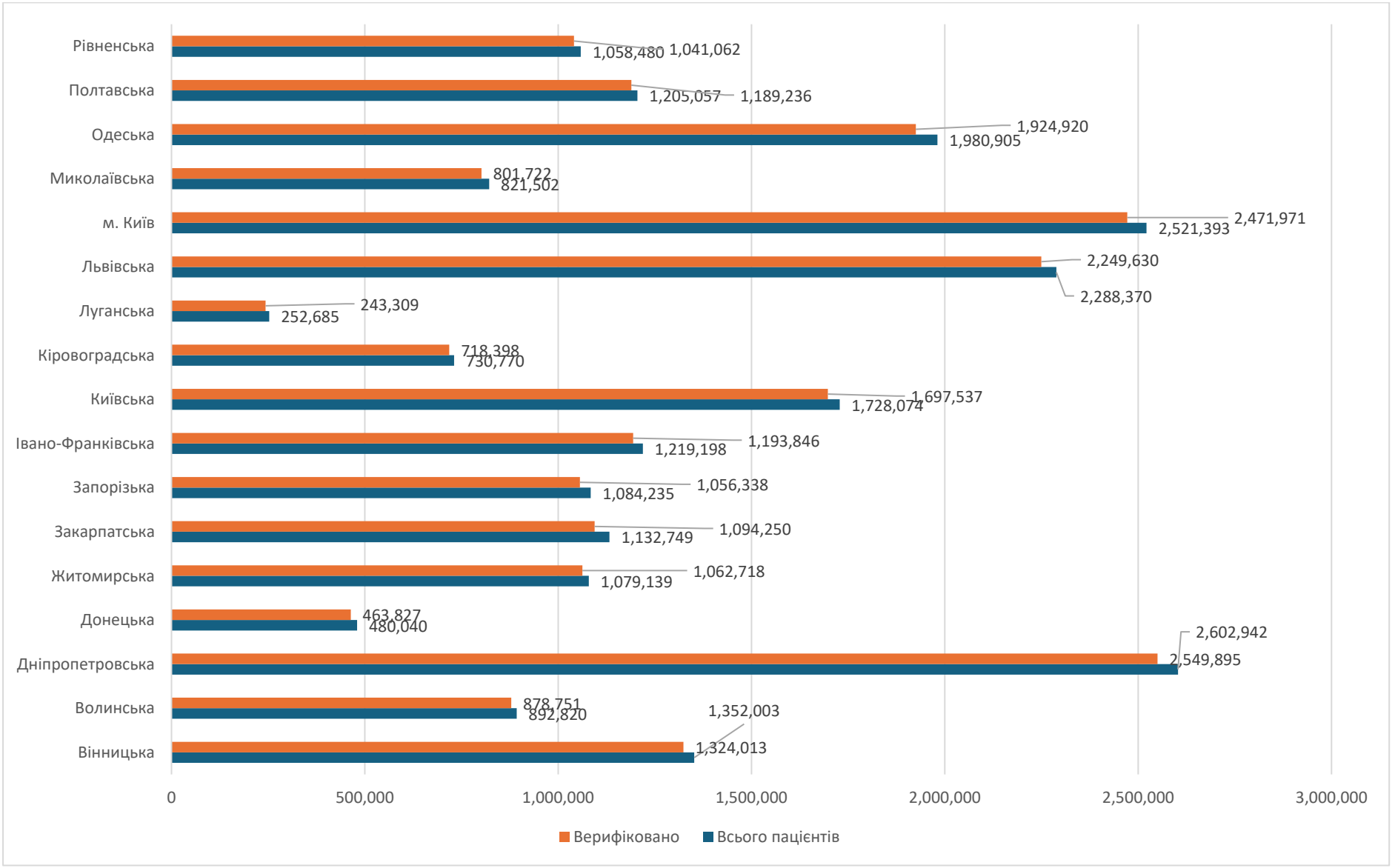


Рис. 3.25. Стан верифікації пацієнтів в електронній системі охорони здоров'я України станом на 2026 рік [17]

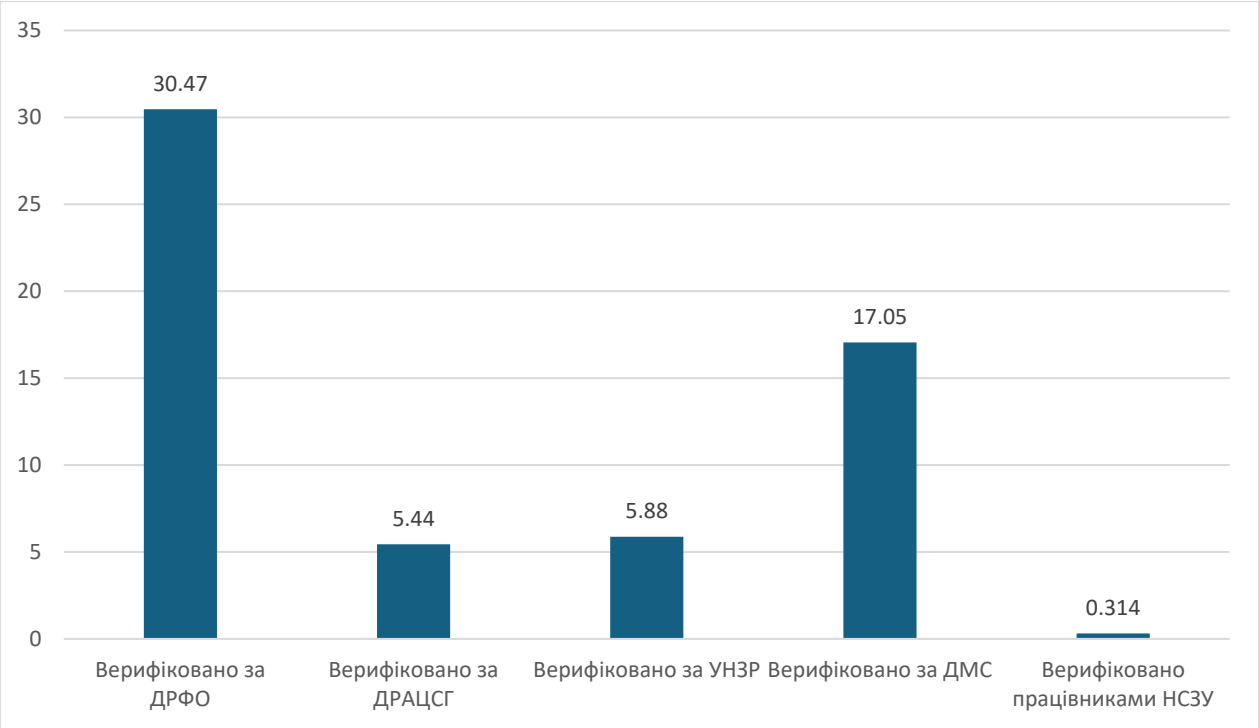


Рис. 3.26. Результати верифікації пацієнтів в електронній системі охорони здоров'я України станом на 2026 рік [17]

Станом на дату формування звіту в електронній системі охорони здоров'я зареєстровано 34,59 млн пацієнтів, з яких 33,55 млн осіб, або 97,0 %, пройшли верифікацію щонайменше за одним із державних реєстрів. Отримані результати свідчать про високий рівень достовірності інформації, що міститься в ЕСОЗ.

Найбільші обсяги верифікації забезпечено через Державний реєстр фізичних осіб – платників податків (ДРФО), за яким підтверджено дані 30,47 млн пацієнтів. Частка верифікованих осіб серед дорослого населення становить 94,7 %, тоді як серед осіб віком до 18 років – 57,5 %.

Через Єдиний державний демографічний реєстр (ЄДДР) підтверджено дані 17,05 млн пацієнтів, що становить 49,3 % від загальної кількості зареєстрованих осіб. За напрямом УНЗР (унікальний номер запису в реєстрі) верифіковано 5,88 млн пацієнтів, а рівень підтвердження даних за цим показником становить 96,4 %.

Крім того, через Державний реєстр актів цивільного стану громадян (ДРАЦСГ) верифіковано 5,44 млн пацієнтів, що охоплює 79,2 % осіб віком до 18 років. Також у системі здійснюється додаткова перевірка даних працівниками НСЗУ, за результатами якої підтверджено понад 34 тис. записів.

Динаміка показника також демонструє поступове зростання кількості верифікованих записів: із 29,1 млн осіб на початку 2025 року до 33,5 млн осіб у 2026 році, що свідчить про постійне вдосконалення механізмів управління даними в електронній системі охорони здоров'я.

Ефективне функціонування електронної системи охорони здоров'я залежить не лише від якості даних пацієнтів, але й від достовірності інформації про медичних працівників. Верифікація медичного персоналу забезпечує коректну ідентифікацію користувачів системи, підвищує рівень інформаційної безпеки та створює необхідні умови для надання цифрових медичних послуг. У зв'язку з цим доцільно проаналізувати результати верифікації записів про медичних працівників в електронній системі охорони здоров'я України на рис. 3.27.

Дані рис. 3.27 свідчать про високий рівень верифікації медичних працівників в електронній системі охорони здоров'я України. Загалом успішну перевірку пройшли 393,3 тис. медичних працівників, тоді як кількість випадків неуспішної верифікації становила 13,1 тис.

Найбільшу кількість успішно верифікованих медичних працівників зафіксовано у місті Києві (53,3 тис.), Львівській (36,7 тис.), Дніпропетровській (30,2 тис.), Харківській (25,7 тис.) та Одеській (21,4 тис.) областях. Такий розподіл пояснюється концентрацією населення, медичних закладів та кадрового потенціалу у великих регіональних центрах.

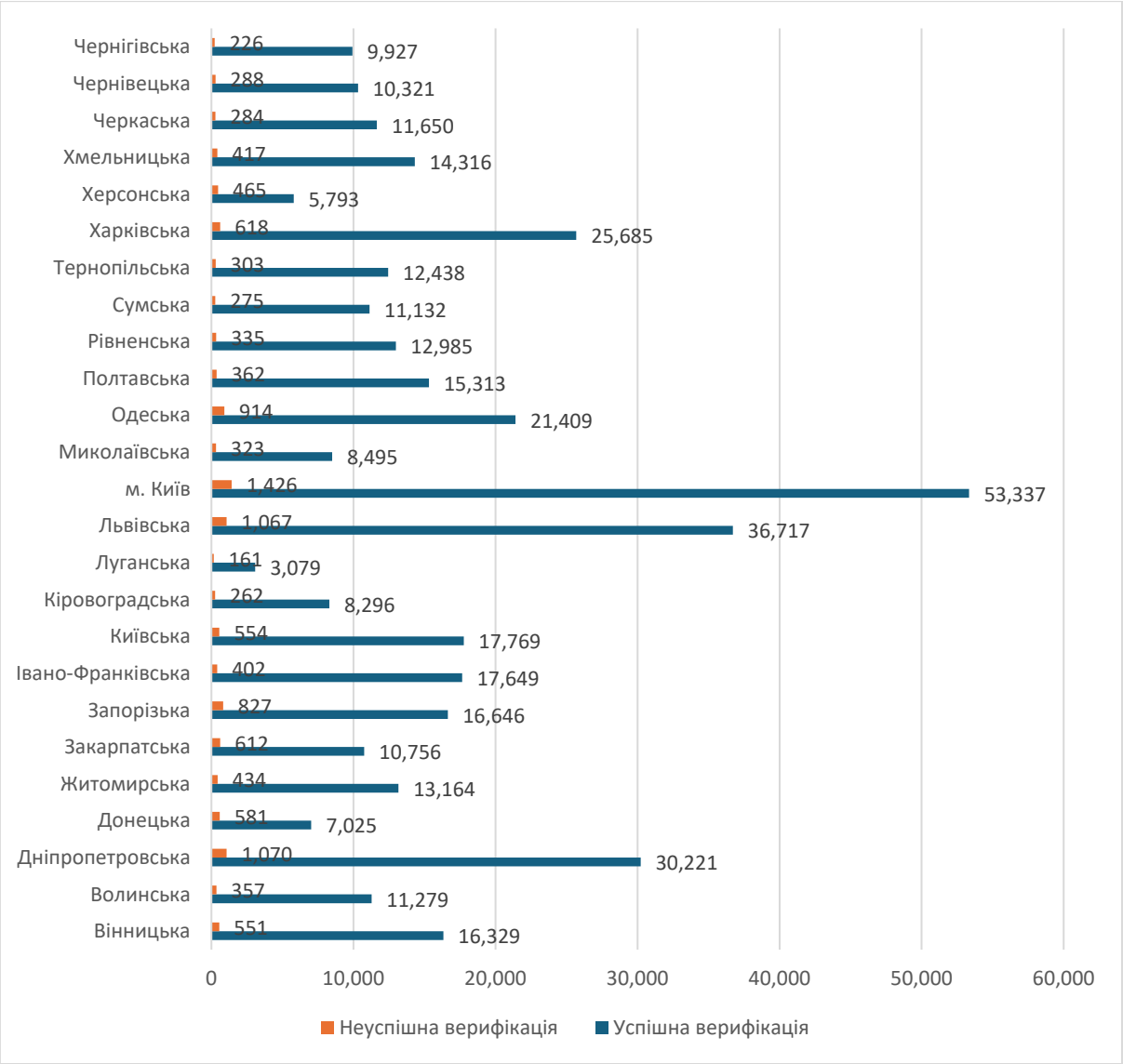


Рис. 3.27. Результати верифікації медичних працівників в електронній системі охорони здоров'я України за регіонами станом на 2026 рік [17]

Кількість медичних працівників, дані яких не пройшли верифікацію, є відносно незначною порівняно із загальним обсягом успішно перевірених записів. Найбільше таких випадків зафіксовано у місті Києві (1 426 осіб), Львівській (1 067 осіб), Дніпропетровській (1 070 осіб) та Одеській (914 осіб) областях.

Водночас лише 17 записів потребують додаткової перевірки, а 10 перебувають у процесі верифікації, що свідчить про практично завершений процес актуалізації кадрових даних у системі.

Високий рівень верифікації пацієнтів і медичних працівників створює основу для ефективного функціонування всієї цифрової екосистеми охорони здоров'я. Водночас важливим елементом її розвитку є інтеграція закладів охорони здоров'я до електронної системи охорони здоров'я, що забезпечує повноцінне надання цифрових медичних послуг на всіх рівнях медичної допомоги. У зв'язку з цим доцільно проаналізувати стан підключення та верифікації закладів охорони здоров'я в Україні на рис. 3.28.

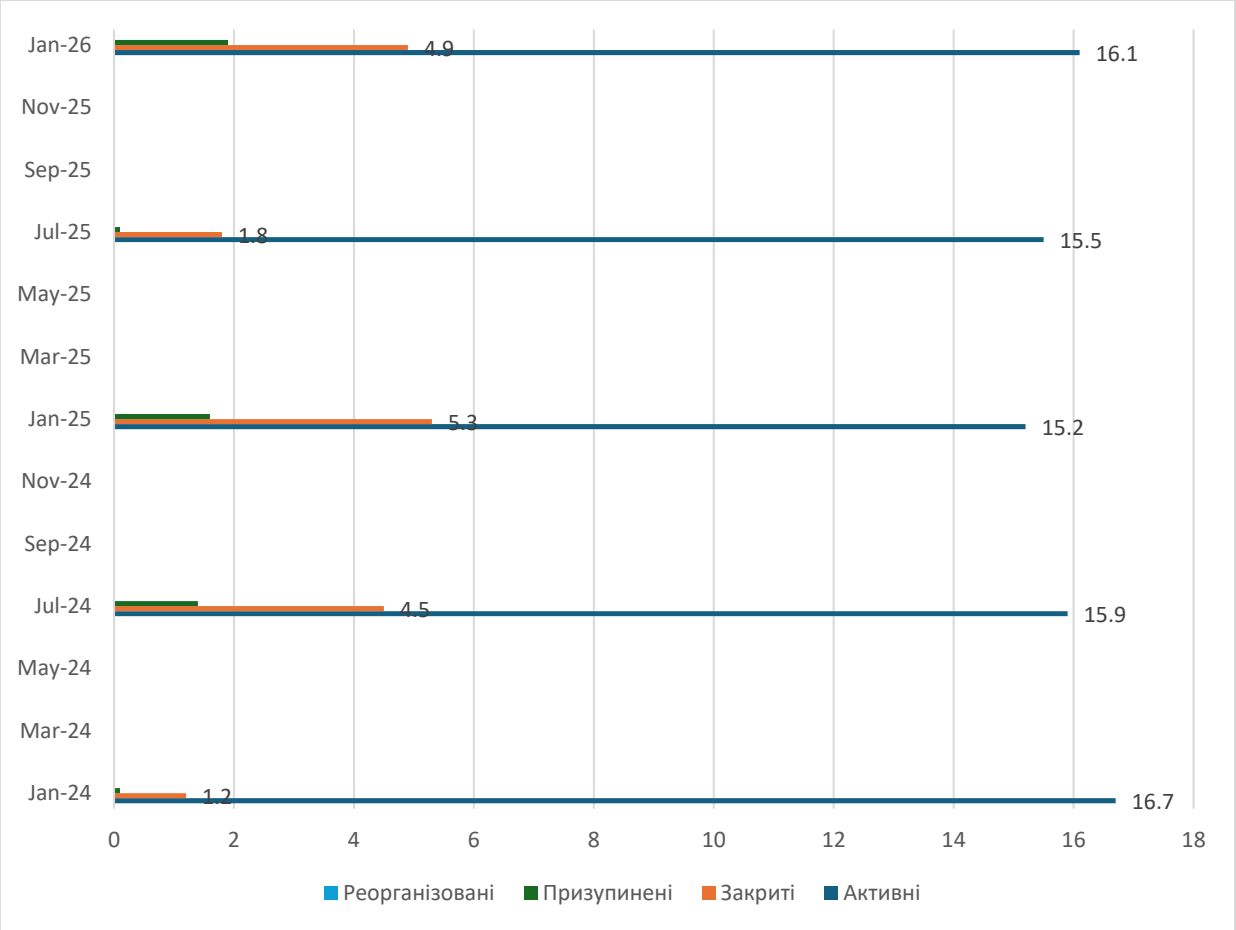


Рис. 3.28. Динаміка кількості суб'єктів господарювання в електронній системі охорони здоров'я України за статусом діяльності у 2024–2026 рр., тис. од. [17]

На наступному рис. 3.29 відображено показники розподілу надавачів медичних та фармацевтичних послуг, підключених до ЕСОЗ, за статусом діяльності та типом закладу станом на 2026 рік, %.

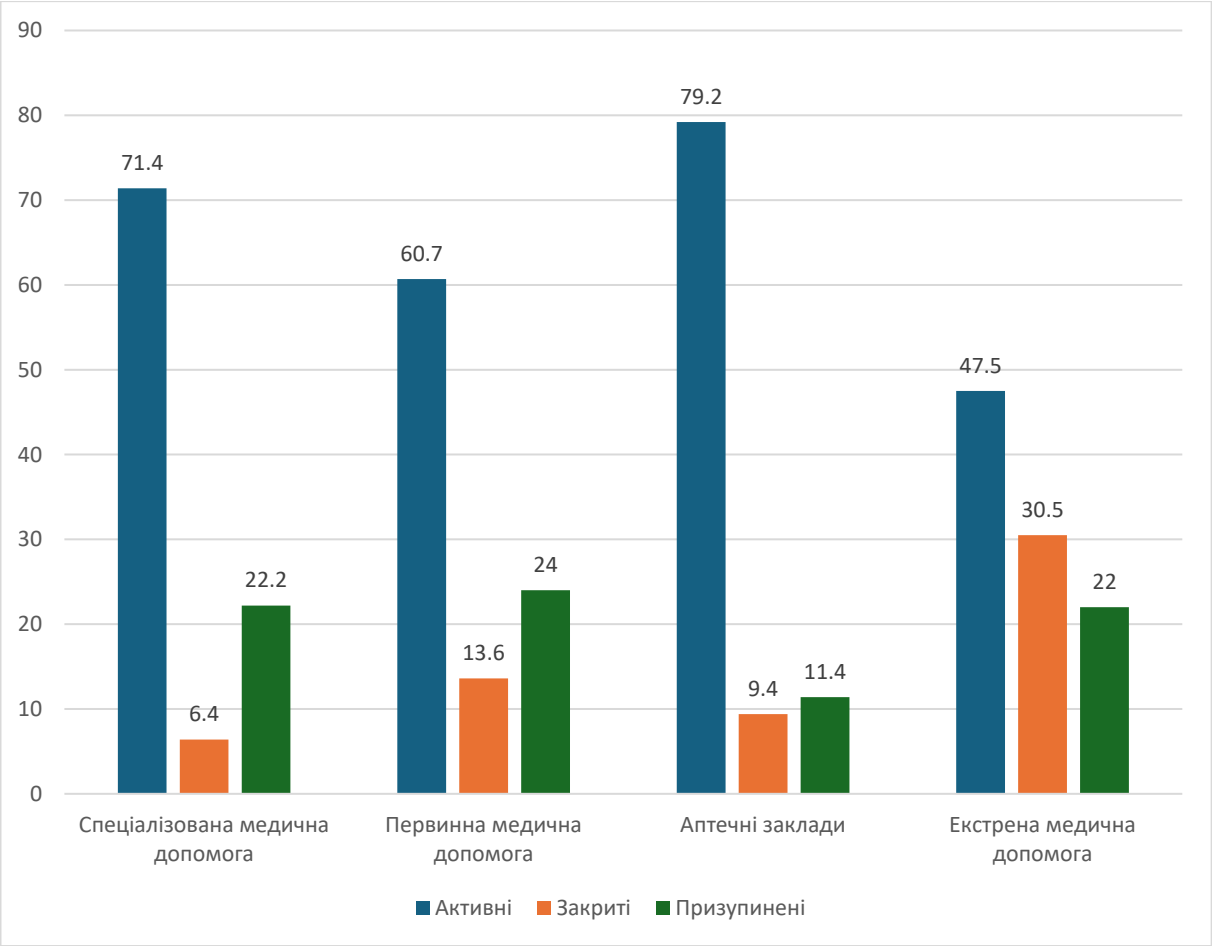


Рис. 3.29. Розподіл надавачів медичних та фармацевтичних послуг, підключених до ЕСОЗ, за статусом діяльності та типом закладу станом на 2026 рік, %[17]

Станом на червень 2026 року в електронній системі охорони здоров'я зареєстровано 23 818 закладів охорони здоров'я та суб'єктів господарювання, з яких 16 781 заклад, або 70,5 %, пройшли процедуру верифікації. Водночас фактичними надавачами медичних послуг є 20 471 суб'єкт господарювання, що свідчить про високий рівень охоплення медичної інфраструктури цифровими сервісами.

Серед зареєстрованих суб'єктів господарювання найбільшу частку становлять активні заклади - 21 602 одиниці, з яких верифіковано 16 545 закладів, або 76,6 %. Частка активних надавачів медичних послуг сягає 18 987 закладів.

Окрему групу становлять закриті заклади, кількість яких становить 16 652 одиниці, з них 16 532 заклади, або 99,3 %, пройшли процедуру верифікації. Також у системі обліковуються 2 108 призупинених закладів, серед яких функції надавачів медичних послуг виконують 1 930 суб'єктів, та 108 реорганізованих закладів охорони здоров'я.

Аналіз структури закладів за видами медичної допомоги показує, що найбільшу частку активних установ мають аптечні заклади, де рівень активності становить 79,2 %. Для спеціалізованої медичної допомоги цей показник дорівнює 71,3 %, для первинної медичної допомоги — 60,7 %, тоді як серед закладів екстреної медичної допомоги частка активних установ становить 47,5 %.

Регіональний аналіз свідчить про найбільшу концентрацію активних закладів у місті Києві (2 166 закладів), Дніпропетровській (1 383), Львівській (1 257) та Одеській (991) областях. Це відповідає демографічному потенціалу регіонів та рівню розвитку медичної інфраструктури.

Важливим підтвердженням успішності цифрової трансформації державного сектору України стало міжнародне визнання з боку Світового банку. За результатами оцінювання цифрової зрілості урядів 198 країн світу у межах індексу GovTech Maturity Index (GTMI) 2025 Україну віднесено до групи A (GovTech Leaders), яка об'єднує держави з найбільш розвиненими та ефективними цифровими рішеннями. Оцінювання здійснювалося за чотирма напрямами: розвиток базових урядових цифрових систем, якість та доступність онлайн-послуг, рівень цифрової участі громадян та наявність інституційних механізмів цифрових змін. Одним із ключових чинників досягнення такого результату стала цифровізація сфери охорони здоров'я. Станом на 2025 рік електронна система охорони здоров'я України охоплювала понад 49 тис. медичних і

аптечних закладів, близько 475 тис. медичних та фармацевтичних працівників, а також понад 5 млрд електронних медичних записів пацієнтів. Це свідчить про формування однієї з найбільших цифрових інфраструктур державного сектору України [72].

Таким чином, результати аналізу декларацій пацієнтів, електронних медичних записів, електронних рецептів, електронних направлень, верифікації пацієнтів, медичних працівників і закладів охорони здоров'я дозволяють комплексно оцінити рівень розвитку цифрової системи охорони здоров'я України та перейти до узагальнення результатів цифрової трансформації галузі.

У результаті проведеного дослідження встановлено, що цифрова трансформація системи охорони здоров'я України є одним із найбільш успішних напрямів модернізації публічного сектору та важливим інструментом підвищення ефективності медичного обслуговування населення. Запровадження електронної системи охорони здоров'я (ЕСОЗ), розвиток цифрових сервісів Національної служби здоров'я України, впровадження електронних декларацій, електронних медичних записів, електронних рецептів та електронних направлень сприяли формуванню єдиного цифрового медичного простору та забезпечили якісно новий рівень взаємодії між пацієнтами, медичними працівниками, закладами охорони здоров'я та державними органами управління.

Отже, здійснений аналіз засвідчив високий рівень охоплення населення цифровими медичними послугами. Станом на 2026 рік найбільша кількість декларацій укладена серед осіб віком 40–64 роки (11,0 млн), тоді як загальна кількість електронних медичних записів зросла з 672 млн у 2022 році до 4,99 млрд у 2025 році, що свідчить про стрімке розширення використання цифрових інструментів у практичній діяльності системи охорони здоров'я.

Важливими результатами цифровізації стало поширення електронних рецептів та електронних направлень. Кількість погашених електронних рецептів зросла з 9,2 млн у 2019 році до 16,2 млн у 2025 році, а кількість створених електронних направлень збільшилася з 20,1 млн у 2020 році до 233,8 млн у 2024 році. Це підтверджує підвищення доступності медичних послуг, прозорості медичних процесів та ефективності управління маршрутами пацієнтів.

Дослідження також показало високий рівень достовірності даних у ЕСОЗ. Верифікацію щонайменше за одним із державних реєстрів пройшли 33,55 млн пацієнтів, що становить 97,0 % від загальної кількості зареєстрованих користувачів системи, а успішно верифікованими є понад 393 тис. медичних працівників. Крім того, цифрова екосистема охоплює понад 23 тис. закладів охорони здоров'я та суб'єктів господарювання, серед яких переважають активні надавачі медичних і фармацевтичних послуг.

Отримані результати свідчать, що в Україні сформовано одну з найбільших цифрових інфраструктур у сфері охорони здоров'я серед країн Європи. Високий рівень цифровізації медичних процесів, масштабність електронних сервісів та міжнародне визнання України серед лідерів цифрової трансформації державного сектору за оцінкою Світового банку підтверджують ефективність реалізованої державної політики у сфері цифрового розвитку охорони здоров'я. Подальший розвиток галузі доцільно пов'язувати з розширенням використання медичних даних, інтеграцією з європейськими цифровими системами охорони здоров'я, розвитком телемедицини, технологій штучного інтелекту та сервісів персоналізованої медицини, що сприятиме підвищенню якості, доступності та безперервності медичної допомоги населенню України.

Висновки до 3-го розділу

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. 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. 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.

РОЗДІЛ 4
ЄВРОІНТЕГРАЦІЙНІ ІМПЕРАТИВИ ДЕРЖАВНОГО УПРАВЛІННЯ ПРОЦЕСАМИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

4.1. Вимоги Європейського Союзу до цифрової трансформації системи охорони здоров’я

Європейський Союз є унікальною міжнародною організацією, органи якої здійснюють регуляторну діяльність, яка є обов’язковою до виконання усіма країнами-членами. Безумовно, що впровадження в національне законодавство положень директив та регламентів Європейського Союзу залежить від особливостей правової та політичної системи тієї чи іншої країни. Система охорони здоров’я в цілому та процеси її цифрової трансформації є пріоритетним та стратегічно важливим завданням регуляторної діяльності Європейського Союзу в соціальній та безпековій сферах. «Рішення щодо охорони здоров’я можуть бути критично важливими, і громадяни Європи повинні відчувати, що їхні дані в безпеці та використовуються з позитивною метою у сфері охорони здоров’я. Дійсно, громадяни ЄС загалом підтримують цифрову охорону здоров’я, причому 80 % погоджуються ділитися своїми медичними даними, якщо гарантовано конфіденційність та безпеку. Тому Європі потрібна правова та етична система управління цифровою охороною здоров'я, яка б відповідала меті та користувалася довірою всіх сторін. Вона повинна збалансувати безпеку та захист даних у контексті переваг для окремої особи та системи охорони здоров'я» [133]. На сьогодні Європейський Союз має важливий досвід в регулюванні процесів цифрової трансформації системи охорони здоров’я, що є вкрай важливим при формуванні вимог для розширення.

Питання цифрової трансформації в Європейському Союзу розглядалися зарубіжними вченими, зокрема: 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), Джонатан Стокс (Jonathan Stokes), 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), 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.

Регуляторна діяльність щодо цифрової трансформації системи охорони здоров'я Європейського Союзу є важливою з наступних причин.

- захист фундаментальних прав на приватність. Цифровізація охорони здоров'я пов'язана з обробкою чутливих персональних даних, тому для ЄС принциповим є забезпечення права людини на приватність, захист персональних даних, інформовану згоду, контроль особи над використанням власної медичної інформації та недискримінаційний доступ до цифрових медичних послуг. Застосування суворих норм (GDPR) гарантує пацієнту повний контроль над власними чутливими даними, захищаючи від їх несанкціонованого використання чи дискримінації. Це забезпечить вирішення сукупності проблем щодо дотримання фундаментальних прав людини. Адже досить часто будь-які реформи в соціально важливих сферах піддаються критиці саме з позиції забезпечення фундаментальних прав людини, які гарантуються міжнародними регламентами та Конституціями країн. Під час розроблення Регламенту про Європейський простір даних охорони здоров'я Європейська рада із захисту даних (EDPB) [153] та Європейський наглядач із захисту даних (EDPS) [152] наголосили, що повторне використання великих масивів медичних даних може створювати ризики для фундаментальних прав людини, якщо не буде забезпечено достатніх гарантій приватності та правової визначеності. Щодо окремих країн, як приклад можна навести досвід Нідерландів при запровадженні електронного обміну медичними даними (Landelijk Schakelpunt, LSP). Так, під час запровадження та розвитку національної системи електронного обміну медичними даними виникла дискусія щодо необхідності належної згоди пацієнтів, обмеження доступу до медичної інформації та контролю особи над використанням її даних, адже була

висока ймовірність порушення права на повагу до приватного життя, захист персональних даних та контролю над власною медичною інформацією. Відповідно було удосконалено систему щодо доступу, оновлення, захисту або видалення медичних записів та даних [107].

- формування та функціонування єдиного регуляторного простору для цифрового ринку охорони здоров'я. Цифровізація є важливою для ЄС, оскільки потребує функціонування єдиного регуляторного простору, в межах якого цифрові медичні послуги, програмне забезпечення, медичні інформаційні системи та цифрові продукти можуть використовуватися за однаковими правилами в усіх державах-членах. Це усуває правові бар'єри, забезпечує вільний рух цифрових медичних рішень та сприяє інтеграції внутрішнього ринку Європейського Союзу. В той же час ринок цифрових рішень стає важливим об'єктом правового регулювання як з боку національного, так і з боку європейського законодавства. Система міжнародного та національного регулювання має забезпечити прозорість, конкуренцію та інноваційність функціонування ринку цифрових рішень для забезпечення безперебійного та ефективного функціонування цифрових систем охорони здоров'я.

- забезпечення транскордонної медичної допомоги через формування єдиного медичного простору. Законодавче створення єдиного цифрового простору (EHDS) дозволяє громадянам вільно пересуватися Європейським Союзом, отримуючи безперервне лікування та доступ до своїх електронних рецептів і медичних даних у будь-якій країні. Європейський Союз створює нормативні та технічні умови для безпечного обміну медичними даними між державами-членами, що забезпечує безперервність медичної допомоги громадянам, взаємне визнання електронних рецептів, доступ до медичної документації та мобільність пацієнтів у межах Союзу.

- посилення кібербезпеки та стійкості цифрової інфраструктури. Медичні інформаційні системи належать до критичної інфраструктури, тому їх захист від кібератак, витоків інформації, несанкціонованого доступу та

інших цифрових загроз є одним із ключових напрямів регуляторної діяльності Європейського Союзу. Регулювання спрямоване на забезпечення безперервності функціонування цифрових медичних сервісів і довіри до них. У 2020 році сталася одна з найбільших у Європі кібератак на медичну установу (психотерапевтичний центр Vastaamo [267]). Було викрадено персональні психотерапевтичні записи десятків тисяч пацієнтів [178], після чого частину постраждалих шантажували, погрожуючи оприлюдненням конфіденційної інформації.

- стимулювання інновацій в розвитку системи охорони здоров'я. Безпечний регульований обмін знеособленими медичними даними через цифрові платформи (вторинне використання даних) відкриває масштабні можливості для дослідників, фармацевтичних компаній та стартапів. Це прискорює розробку нових ліків, персоніфікованої медицини та рішень на основі штучного інтелекту всередині ЄС. В даному контексті варто навести досвід Естонії [181] щодо Геномного дослідження EstBB, коли було оцифровано геномні дані понад 200 000 громадян (понад 20 % дорослого населення) та інтегровано ці дані безпосередньо в картки лікаря. Інновація дозволила лікарям первинної ланки автоматично розраховувати індивідуальні полігенні ризики (PRS) для кожного пацієнта щодо серцево-судинних захворювань та раку грудей, а також коригувати дозування ліків на основі фармгеноміки ще до прояву симптомів. Щодо Німеччини [112], то у рамках Закону про цифрове постачання (DVG) Німеччина створила перший у світі прозорий правовий механізм Fast-Track, який дозволяє лікарям виписувати рецепт на мобільний застосунок (наприклад, для когнітивно-поведінкової терапії, контролю діабету чи реабілітації), а державній страховці повністю покривати його вартість. Це створило бурхливий ринок медтех-стартапів. Понад 50 цифрових продуктів пройшли клінічну валідацію та отримали офіційну сертифікацію, давши поштовх розвитку доказової цифрової терапевтики.

- безпечне та етичне впровадження штучного інтелекту в медицину. Технології штучного інтелекту в діагностиці, аналізі медичних зображень та розробці ліків потребують величезних масивів якісних, стандартизованих та уніфікованих цифрових даних. Без чіткого законодавчого регулювання існує ризик використання недостовірних або викривлених даних, що може призвести до лікарських помилок, алгоритмічної дискримінації чи витоку таємниць. Регульована цифрова трансформація дозволяє Європейському Союзу створити безпечне середовище для навчання медичного штучного інтелекту з обов'язковим людським контролем, високою точністю та прозорістю алгоритмів. Зазначимо, що в оприлюднених результатах досліджень [228] зазначено, що у кількох країнах ЄС під час тестування алгоритмів для розподілу медичних ресурсів та визначення пріоритетності лікування експерти звертали увагу на ризики алгоритмічної дискримінації, коли рішення могли бути недостатньо зрозумілими або містити упередження щодо окремих груп пацієнтів. У 2026 році Європейський економічний і соціальний комітет зазначив, що штучний інтелект, навчений переважно на даних чоловіків європейського походження, може частіше помилятися під час діагностики жінок, а також посилювати вже існуючі гендерні нерівності у сфері охорони здоров'я. Подібна інформація міститься у дослідженні Європейського Парламенту Artificial Intelligence in Healthcare [99], зокрема наведено приклади, коли алгоритми можуть: приймати менш точні рішення щодо окремих груп населення; відтворювати дискримінацію, яка вже існувала в навчальних даних; формувати необґрунтовані клінічні рекомендації без можливості їх пояснення.

- підвищення ефективності державного управління стійкістю та активністю системи охорони здоров'я. Використання цифрових технологій дозволяє оптимізувати адміністративні процеси, покращити планування ресурсів, моніторинг стану здоров'я населення та реагування на

надзвичайні ситуації, що особливо проявилося під час пандемії COVID-19. Цифровізація забезпечує накопичення якісних даних про стан здоров'я населення, ефективність медичних технологій та результати лікування. Це дозволяє інституціям Європейського Союзу приймати регуляторні рішення на основі достовірних даних, прогнозувати потреби системи охорони здоров'я та своєчасно реагувати на кризові ситуації, зокрема пандемії чи демографічні виклики. Крім того, дублювання обстежень, паперова бюрократія та медичні помилки через відсутність даних є досить витратними для Європейського Союзу – мільярди євро щороку. Цифрова трансформація дозволяє уніфікувати стандарти, оптимізувати витрати та зробити національні системи охорони здоров'я стійкішими до нових пандемій чи масштабних криз.

Зазначені причини стали передумовою формування нормативно-правового поля цифрової трансформації системи охорони здоров’я в Європейському Союзі. Формування системи нормативного регулювання відбувалося еволюційним шляхом та пройшло декілька етапів, що пов’язано не лише з політичними та правовими аспектами, але й технічними, технологічними, соціальними, економічними та медичними. Так, будь-які інноваційні рішення техніко-технологічного характеру вимагають їх врегулювання з позиції впровадження в медицину та управління системою охорони здоров’я. В той же час цифрова трансформація є ресурсномістким та фінансово-затратним процесом, а відповідно будь-які економічні зміни спричиняють можливість держави забезпечувати процеси цифрової трансформації системи охорони здоров’я.

Еволюція процесів цифрової трансформації в Європейському Союзі відбувалася з 1990-х років та має на сьогодні ряд результатів. Вивчивши наукову літературу, можна виділити наступні етапи цифрової трансформації системи охорони здоров’я в Європейському Союзі (рис. 4.1).

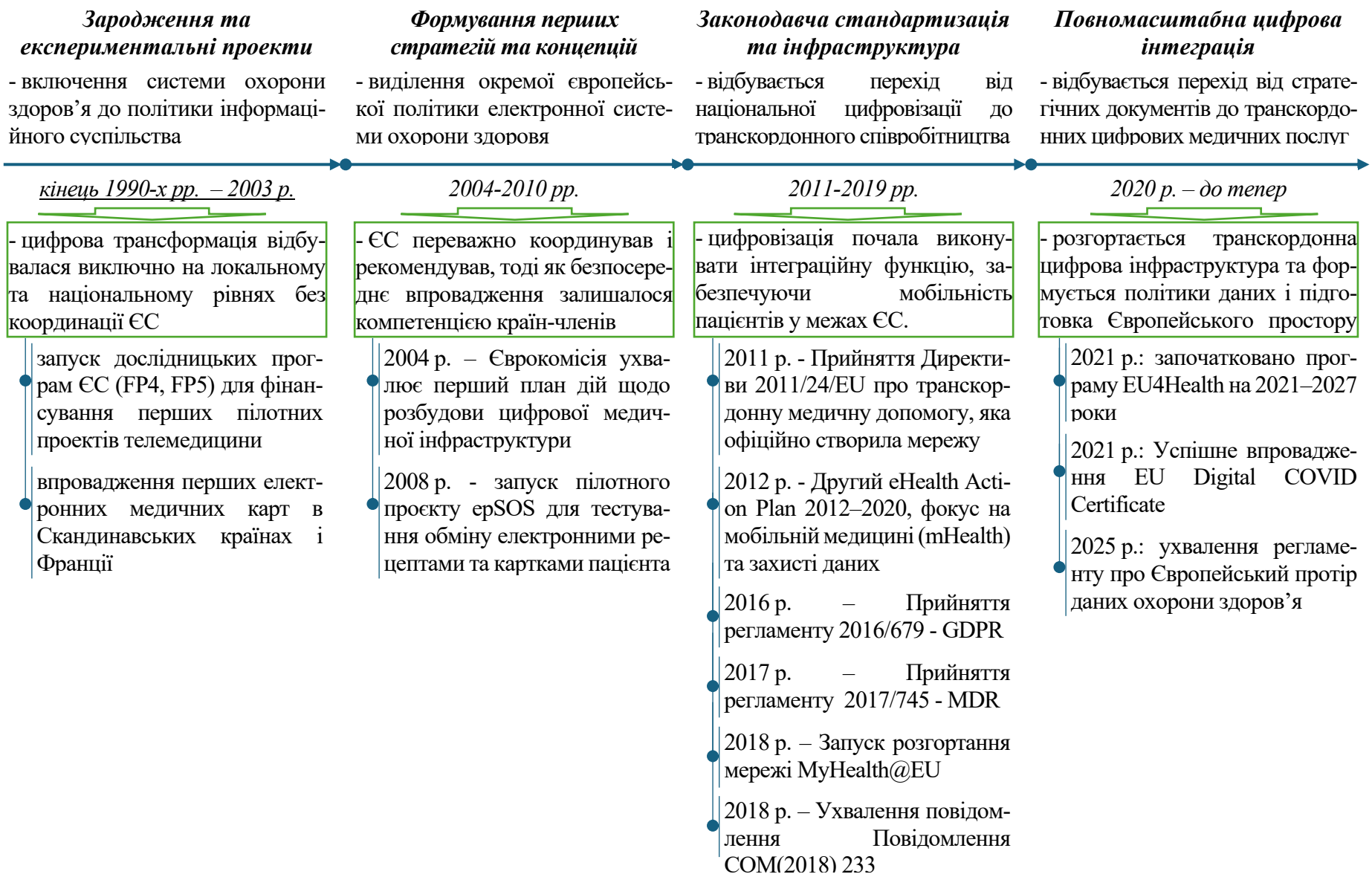


Рис. 4.1. Еволюція системи регулювання Європейським Союзом процесів цифрової трансформації системи охорони здоров'я

Перший етап еволюції системи регулювання процесів цифрової трансформації системи охорони здоров'я припадає на період з кінця 1990-х років по 2003 р. Пропонуємо розглядати даний етап як етап зародження та експериментальних проектів, на якому відбуваються перші спроби включення системи охорони здоров'я до політики інформаційного суспільства. Цифрові рішення впроваджувалися фрагментарно лише на локальних та в окремих країнах національному рівнях, а стосувалися вони переважно: комп'ютеризації закладів охорони здоров'я; створення електронних баз медичної інформації; розвитку телемедицини; забезпечення доступу медичних установ до інтернету; формування початкових вимог до сумісності інформаційних систем.

Другий етап - формування перших стратегій та концепцій припадає на 2004-2010 рр. та визначається тим, що цифрова трансформація системи охорони здоров'я виділяється Європейським Союзом в окрему політику. Початком даного етапу вважається затвердження Єврокомісією першого плану дій в сфері електронної системи охорони здоров'я. Відтак державам-членам було запропоновано: розробляти національні та регіональні дорожні карти електронної охорони здоров'я; запроваджувати електронні медичні записи; розвивати електронні рецепти; визначати спільні підходи до ідентифікації пацієнтів; формувати стандарти обміну медичними повідомленнями; забезпечувати інтероперабельність медичних інформаційних систем; уточнювати правове регулювання телемедицини та захисту персональних даних. У 2008 р. відбувся запуск пілотного проекту epSOS для тестування обміну електронними рецептами та стислими картками пацієнта між різними країнами.

Третій етап припадає на 2011-2019 рр., який можна назвати «Законодавча стандартизація та інфраструктура». У ці роки відбувається перехід від національної цифрової трансформації до транскордонного співробітництва, а цифрова трансформація почала виконувати інтеграційну функцію, забезпечуючи мобільність пацієнтів у межах Європейського Союзу. У цей період цифрова трансформація почала безпосередньо пов'язуватися з реалізацією права

громадян ЄС на отримання медичної допомоги в іншій державі-члені. Основними напрямами стали: транскордонний обмін електронними рецептами; створення електронного резюме пацієнта; взаємне визнання медичної інформації; розроблення спільної термінології та форматів даних; формування національних контактних пунктів електронної охорони здоров'я; технічна й організаційна сумісність національних систем. Ключовими подіями даного періоду стали: прийняття Директиви 2011/24/EU про транскордонну медичну допомогу, яка офіційно створила мережу; другий eHealth Action Plan 2012–2020, фокус на мобільній медицині (mHealth) та захисті даних; прийняття регламенту 2016/679 – GDPR; прийняття регламенту 2017/745 – MDR; запуск розгортання мережі MyHealth@EU; ухвалення Повідомлення COM(2018) 233.

Повномасштабна цифрова інтеграція як етап еволюції системи регулювання ЄС процесів цифрової трансформації системи охорони здоров'я розпочався у 2020 році та продовжується й надалі. Значним каталізатором змін стала пандемія COVID-19, яка висвітлила критичну потребу в миттєвому обміні даними та єдиних стандартах. На даному етапі відбувається перехід від стратегічних документів до транскордонних цифрових медичних послуг. Розгортається транскордонна цифрова інфраструктура та формується політика даних і підготовка Європейського простору даних охорони здоров'я. Через сформовану структуру стало можливим здійснювати обмін електронними рецептами, інформацією про відпуск лікарських засобів, електронними резюме пацієнтів. У цей період в політику цифрової трансформації включено питання з реалізації права громадян ЄС на отримання медичної допомоги в іншій державі-члені, що обумовило розвиток: транскордонного обміну електронними рецептами; електронного резюме пацієнта; взаємного визнання медичної інформації; спільної термінології та форматів даних; національних контактних пунктів електронної охорони здоров'я; технічної й організаційної сумісності національних систем. Таким чином, цифрова трансформація почала розглядатися як інструмент пацієнтоцентричності, персоналізованої медицини та доказової політики.

У результаті еволюції регулювання цифрової трансформації системи охорони здоров'я Європейським Союзом на сьогодні сформувалася цілісна система нормативно-правових актів, які можна структурувати наступним чином (рис. 4.2). Більш детально характеризуємо зазначені нормативно-правові акти.

До ***базових регуляторних документів*** належать:

1. Регламент (ЄС) 2025/327 про Європейський простір даних охорони здоров'я (EHDS) (Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847) [248]. Даний Регламент був ухвалений 11 лютого 2025 року та на даний час є ключовим нормативно-правовим актом Європейського Союзу щодо цифрової трансформації системи охорони здоров'я, а його метою є створення єдиного європейського правового та інформаційного простору медичних даних. «Метою цього Регламенту є створення Європейського простору даних охорони здоров'я (EHDS) з метою покращення доступу фізичних осіб до своїх персональних електронних даних про здоров'я та контролю над ними в контексті охорони здоров'я, а також для кращого досягнення інших цілей, пов'язаних з використанням електронних даних про здоров'я в секторах охорони здоров'я та догляду, які принесуть користь суспільству, таких як дослідження, інновації, розробка політики, готовність до загроз здоров'ю та реагування на них, включаючи запобігання та подолання майбутніх пандемій, безпека пацієнтів, персоналізована медицина, офіційна статистика або регуляторна діяльність. Крім того, метою цього Регламенту є покращення функціонування внутрішнього ринку шляхом встановлення єдиної правової та технічної бази, зокрема для розробки, маркетингу та використання систем електронних медичних записів («системи EHR») відповідно до цінностей Союзу. EHDS буде ключовим елементом у створенні сильного та стійкого Європейського союзу охорони здоров'я» [248].

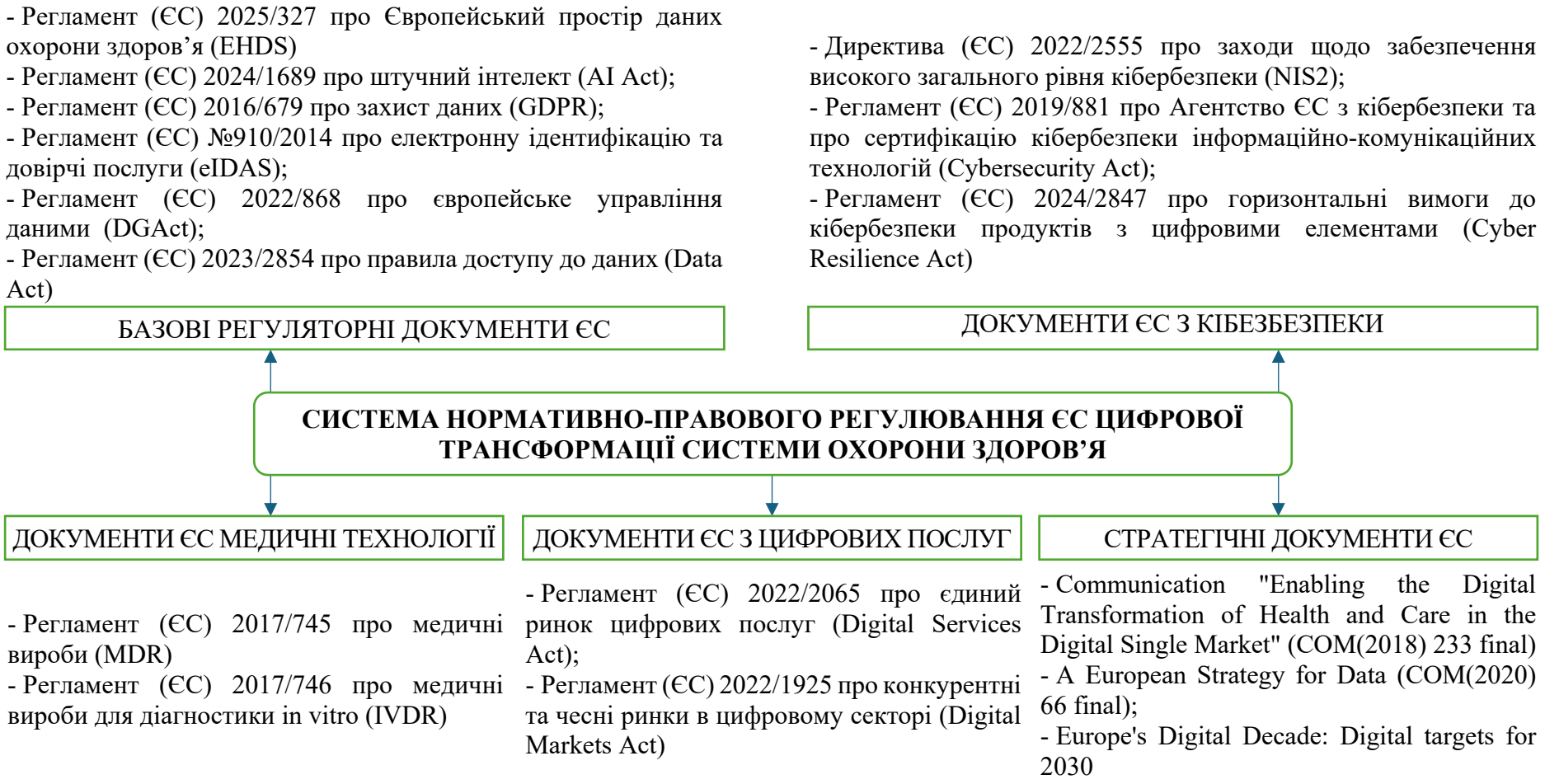


Рис. 4.2. Структура системи нормативно-правових актів Європейського Союзу, що регулюють цифрову трансформацію системи охорони здоров'я

Прийняття Регламенту (ЄС) 2025/327 стало переходом від фрагментарної цифрової трансформації національних систем охорони здоров'я та координаційної взаємодії держав-членів до формування єдиного регуляторного, інформаційного й технологічного простору охорони здоров'я ЄС, заснованого на інтероперабельності електронних медичних даних, гарантуванні прав пацієнта та можливості їх транскордонного і вторинного використання. Відповідно регламент має декілька ключових напрямів регулювання:

- по-перше, посилення прав пацієнта на власні медичні дані, виходячи з чого пацієнт стає не лише об'єктом накопичення медичних даних, а розпорядником цих даних (статті 3, 7, 8 та 9). Так, положення Регламенту визначають простішу процедуру отримання електронного доступу до власних медичних даних, їх завантаження та контролю доступу користувачами під час отримання медичної допомоги;

- по-друге, формування правового поля функціонування інфраструктури MyHealth@EU для транскордонного обміну медичними даними між країнами ЄС (статті 14, 15, 16, 23 та 24). Дана інфраструктура забезпечує здійснення обміну електронними рецептами, резюме пацієнта, медичними зображеннями, лабораторними результатами, випісками із закладів охорони здоров'я та іншими даними;

- по-третє, встановлення єдиних вимог до електронних систем медичних записів, які використовуються в державах-членах ЄС (статті 49-78). Він визначає вимоги щодо інтероперабельності, безпеки, структури даних, технічної документації, сертифікації та функціональної сумісності програмного забезпечення;

- по-четверте, врегулювання механізму вторинного використання медичних даних (статті 61, 67, 68, 69, 73, 74) для наукових досліджень; розроблення інновацій; статистики; формування державної політики; діяльності регуляторних органів; оцінювання медичних технологій; навчання та перевірки алгоритмів штучного інтелекту;

- по-п’яте, формування системи державного та наднаціонального управління цифровими медичними даними (статті 97, 98, 99, 100, 101) через утворення національних органів цифрової охорони здоров’я, органів доступу до медичних даних, Ради EHDS, європейські цифрові інфраструктури MyHealth@EU та HealthData@EU.

Критичні положення даного регламенту були розглянуті в працях зарубіжних вчених, зокрема: Лука Мареллі та інші [207] вказують на надмірну централізацію і послаблення контролю пацієнта; Річард Рак (Richard Rak) [235] визначає ризики приватності при вторинному використанні, адже EHDS передбачає масштабне вторинне використання медичних даних, включаючи великі масиви персональних та неперсональних даних; Едвард С. Дав (Edward S. Dove) [138] обґрунтовує зміст конфлікту між інноваціями та етикою; Сюсінь Яо (Xuxin Yao), Чжеюань Сунь (Zheyuan Sun) та Хунцзе Ман (Hongjie Man) [282] вказують на проблему балансування наукових та комерційних інтересів; Jane Arroyo (Джейн Арройо), Hien Vu (Хієн Ву), Timothy Yu-Cheong Yeung (Тімоті Ю-Чонг Йонг) [97].

Станом на сьогодні Україною вже створено базові організаційні, інформаційні та технологічні передумови для наближення до вимог Європейського простору даних охорони здоров’я. До них належать: створення електронної системи охорони здоров’я; запровадження електронних медичних записів, електронних рецептів та електронних направлень; функціонування централізованої цифрової інфраструктури; використання медичних даних для державного управління та адміністрування системи охорони здоров'я; а також формування інституційної системи управління цифровою трансформацією галузі. Проте для повного приведення у відповідність із досліджуваним регламентом є потреба в: 1) гармонізації національного законодавства в частині прав пацієнтів на доступ до електронних медичних даних, їх перенесення, виправлення, обмеження доступу до них та контролю за їх

використанням; 2) створенні механізму транскордонного обміну електронними медичними даними шляхом забезпечення технічної та нормативної сумісності; 3) досягненні повної інтероперабельності електронної системи охорони здоров'я відповідно до технічних специфікацій ЄС; 4) нормативному врегулюванні вторинного використання медичних даних; 5) визначенні компетентного органу з питань цифрової охорони здоров'я, органу доступу до медичних даних, а також механізмів взаємодії з європейськими цифровими інфраструктурами та інституціями.

2. Регламент (ЄС) 2024/1689 про штучний інтелект (AI Act) (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)) [246]. Регламент був ухвалений 12 липня 2024 року та набрав чинності 1 серпня 2024 року. Даним регламентом встановлено: по-перше, єдині правила використання технологій штучного інтелекту в медицині (статті 1, 5 та 6); по-друге, віднесення більшості медичних AI-систем до категорії високого ризику (статті 6, додаток I та III); по-третє, механізм захисту фундаментальних прав людини (статті 5, 13, 14 та 27); по-четверте, механізм інформування пацієнтів про використання штучного інтелекту (статті 13, 15 та 16); по-п’яте, механізм створення системи державного нагляду (статті 64-70). Таким чином, якщо EHDS визначає правила доступу, обміну та використання електронних медичних даних, то AI Act встановлює вимоги до безпечного, прозорого та правомірного використання штучного інтелекту, який використовує ці дані для діагностики, лікування, прогнозування та підтримки прийняття медичних рішень.

Проблемними аспектами впровадження даного регламенту, на яких наголошували вчені, є наступними: надмірна складність та ризик регуляторного перевантаження (Нуну Соуза е Сілва (Nuno Sousa e Silva) [257]); надмірно орієнтований на класифікацію та управління ризиками, але недостатньо враховує конкретні фундаментальні права, які можуть бути порушені (Ніколетта Рангоне (Nicoletta Rangone), Лука Мегале (Luca Megale) [236]); не враховує контекст застосування технологій штучного інтелекту, а лише характеристики системи (Мартін Еберс (Martin Ebers) [140]); регламент намагається протидіяти дискримінації, але недостатньо враховує структурні джерела (Анастасія Караджанні (Anastasia Karagianni) [184]); реалізація потребує значної інституційної та експертної спроможності (Клаудіо Новеллі (Claudio Novelli), Філіп Хакер (Philipp Hacker), Джессіка Морлі (Jessica Morley), Ярле Трондал (Jarle Trondal), Лучано Флоріді (Luciano Floridi) [222]).

Питання використання штучного інтелекту в медицині та й в інших соціально важливих та безпекових сферах суспільного життя є вкрай важливим і на сьогодні має бути врегульованим. Причому при формуванні правового поля використання технологій штучного інтелекту необхідно передбачати сукупність норм, які регулюють постійну динамічність оновлення законодавства, що дасть можливість приведення його у відповідність до розвитку науки і технологій.

3. Регламент (ЄС) 2016/679 про захист даних (GDPR) (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)) [238] є базовим нормативно-правовим актом Європейського Союзу у сфері захисту персональних даних, який був ухвалений 27 квітня 2016 року, а набрав чинності 24 травня 2016 року, а

застосовується з 25 травня 2018 року. «Розширення обсягу медичних даних пропонує захопливі можливості для підтримки кращого та ефективнішого пошуку, розробки та впровадження ліків. Захист даних та управління забезпечують правову основу для балансу між захистом конфіденційності пацієнтів та перевагами медичних досліджень для суспільства» [121]. В даному документі містяться положення, що визначають: по-перше, правові засади обробки персональних медичних даних (статті 5, 6 та 9); по-друге, посилення прав суб'єкта персональних даних (статті 12, 13, 14, 15, 16, 17, 18, 20, 21); по-третє, захист даних за замовчуванням і під час проєктування цифрових систем (стаття 25); по-четверте, забезпечення безпеки обробки персональних даних (статті 32, 33, 34); посилення підзвітності та державного контролю (статті 5, 24, 51-59, 83).

В умовах євроінтеграції державна політика цифрової трансформації національної системи охорони здоров’я України, має передбачати: гармонізацію законодавства про захист персональних даних; запровадження принципу Privacy by Design та Privacy by Default при створенні цифрових медичних систем; посилення прав пацієнтів щодо доступу до власних медичних даних; удосконалення механізмів кібербезпеки та реагування на порушення захисту даних; зміцнення інституційної спроможності незалежного органу із захисту персональних даних.

Регламент (ЄС) 2016/679 про захист даних (GDPR) передбачає значне удосконалення правового поля цифрової трансформації системи охорони здоров’я в Європейському Союзі, але й в той же час має ряд недоліків, на яких наголошували вчені. Зокрема, Джулі-Енн (Julie-Anne R. Smit), Менно Мостерт (Menno Mostert), Ріке ван дер Грааф (Rieke van der Graaf), Дідерік Е. Гроббі (Diederick E. Grobbee), Йоганнес Дж. М. ван Дельден (Johannes J. M. van Delden) вказують, що «Поширеним непорозумінням є чинне

європейське законодавство про захист даних, що коли згода не використовується як законна підстава, обробка персональних даних заборонена. Стаття 9(2)(j) Загального регламенту про захист даних ЄС (GDPR) дозволяє державам-членам встановити правову основу в національному законодавстві, яка дозволяє обробку персональних даних для наукових дослідницьких цілей без їхньої згоди. Однак європейський законодавець сформулював це «виключення для досліджень» як вступне положення, що робить GDPR неконкретним щодо того, які саме заходи необхідні для дотримання виключення для досліджень. Це може мати значні наслідки як для захисту персональних даних, так і для розвитку досліджень у сфері охорони здоров'я з інтенсивним використанням даних» [256].

Аманда Коул (Amanda Cole), Адріан Тоуз (Adrian Towse) [121] в своєму дослідженні наголошують на невизначеності щодо застосування положень регламенту, що може призвести до сукупності проблем, що пов’язані з невизначеністю щодо: правових підстав обробки даних без згоди; наукових досліджень; вторинного використання даних; анонімізації; сумісності первинного і вторинного використання; різного тлумачення правил у державах-членах.

Державно-управлінська точка зору в контексті впровадження процедур визначених регламентом в конкретній державі міститься в публікації Мікаель Паасо (Mikael Paaso) [230]. Вчений зазначає, що після запровадження GDPR зросла потреба в працівниках, пов’язаних із compliance та збільшилася кількість завдань, пов'язаних із захистом даних. В публікації наводяться результати дослідження, що підтверджують вплив регуляторних витрат GDPR на розвиток бізнесу в сфері цифровізації. «після впровадження GDPR стартапи, що працюють з великим обсягом даних, в ЄС зростали повільніше порівняно з їхніми американськими аналогами» [230].

Варто зазначити, що критика положень Регламенту (ЄС) 2016/679 про захист даних (GDPR) звучала з боку офісу Європейського інспектора із захисту даних [278], де було зазначено, що попри безпосередню застосовність GDPR у всіх державах-членах, Регламент залишає державам значний простір для встановлення додаткових умов щодо обробки спеціальних категорій даних. В першу чергу це стосується медичних даних і наукових досліджень, що може призводити до регуляторної фрагментації та створювати різні умови для транскордонного використання медичних даних у Європейському Союзі. Крім того, в документі ставиться під сумнів припущення, що збільшення доступності даних автоматично створює суспільну користь, і аналізують ризик послаблення фактичного контролю пацієнта над даними.

Зазначені критичні положення Регламент (ЄС) 2016/679 про захист даних (GDPR) впливають на державну євроінтеграційну політику та політику цифрової трансформації України і в усіх сферах суспільного життя, зокрема системи охорони здоров'я. При реалізації зазначених політик, варто врахувати думку вчених та сформувати комплекс заходів для кадрового, фінансового, безпекового та інфраструктурного забезпечення реалізації Регламенту (ЄС) 2016/679 про захист даних (GDPR), налагодити співпрацю з країнами-членами ЄС щодо транскордонного вторинного використання медичних даних та забезпечити захист персональних даних, які використовуються для наукових досліджень.

4. Регламент (ЄС) №910/2014 про електронну ідентифікацію та довірчі послуги (eIDAS) (Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework) [245]. Регламент встановив загальноєвропейські правила щодо електронної ідентифікації та довірчих послуг для електронних транзакцій. Для

цифрової системи охорони здоров'я його значення полягає насамперед у тому, що він створює правові механізми надійної ідентифікації пацієнта та медичного працівника, автентифікації, електронного підпису та підтвердження справжності електронних документів.

Регламентом передбачено:

- по-перше, правову основу для взаємного визнання засобів електронної ідентифікації між державами-членами;

- по-друге, встановлення правил використання електронних підписів та визначає правові наслідки їх застосування;

- по-третє, використання електронних печаток юридичних осіб, які дозволяють підтвердити походження та цілісність електронних документів;

- по-четверте, регулювання електронної позначки часу.

На сьогодні в Україні для відповідності зазначеному документу створено базове законодавство про електронну ідентифікацію та довірчі послуги (Закон України № 2155-VIII «Про електронну ідентифікацію та електронні довірчі послуги» [42]), яким передбачено: модернізацію українського регулювання електронної ідентифікації та довірчих послуг наближеного до норм ЄС; функціонування системи кваліфікованих електронних підписів і печаток; запровадження рівнів довіри електронної ідентифікації; розвиток нормативної бази цифрових гаманців.

В той же час необхідне забезпечення повної правової та технічної сумісності української системи електронної ідентифікації з оновленою системою eIDAS 2.0, включаючи взаємне транскордонне визнання засобів електронної ідентифікації та довірчих послуг, сумісність цифрових гаманців і можливість їх використання для доступу до європейських цифрових сервісів.

Зміст та реалізація даного регламенту неодноразово розглядалася вченими з позиції правових, технологічних та організаційних проблем. Іван Абеллан Альварес (Iván Abellán Álvarez), Пол Гельцмер (Pol Hölzme), Йоганнес Седлмайр (Johannes Sedlmeir) [83] вважають, що положення регламенту не дозволяють уникнути ризику надмірного розкриття персональних даних. Проблема стає особливо чутливою, якщо через цифровий гаманець використовуються: медична страховка; підтвердження права на медичну допомогу; рецепти; медичні атрибути; документи пацієнта. Крім того, автори наголошують, що через різні механізми цифрової ідентифікації виникає потенційна можливість пов'язування інформації з різних сфер життя людини.

На проблемі реального контролю людини над цифровою ідентичністю наголошує Сара Гарсія (Sara Garsia) [159], адже авторка ставить під сумнів, чи справді її впровадження відповідає цінності автономії як мети конфіденційності та захисту даних, зокрема відповідно до GDPR та Хартії основних прав ЄС. Це дозволяє авторці зробити висновок, що формальний контроль над цифровою ідентичністю не гарантує фактичної автономії особи, що особливо актуально для пацієнтів, які можуть мати недостатні цифрові навички або залежати від інших осіб при користуванні цифровими послугами.

Марте Ейдсанд Кйорвен (Marte Eidsand Kjørven), Крістіан Гьостен (Kristian Gjøsteen), Тон Лінн Верстад (Tone Linn Wærstad) [186] наголошують на проблемі особистого контролю над особистими даними, зокрема автори наголошують, що «Регламент eIDAS 2.0 зобов'язує всі держави-члени забезпечити громадян Європейським цифровим гаманцем ідентифікації (EDIW). Центральним принципом, що лежить в основі цієї системи, є одноосібний контроль, який гарантує, що використання EDIW, а також електронних посвідчень особи та підписів, може бути пов'язане з

їхніми законними користувачами. Хоча криптографічне розуміння одноосібного контролю зосереджено на технічних заходах безпеки, його реальне застосування є набагато складнішим. Практичний контроль над власною цифровою ідентичністю часто недоступний для осіб з обмеженими цифровими навичками, інвалідністю або для тих, хто покладається на допомогу третіх сторін. Інші можуть стати жертвами шахрайства, примусу або атак соціальної інженерії» [186].

5. Регламент (ЄС) 2022/868 про європейське управління даними (DGAct) (Regulation (EU) 2022/868 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)) був ухвалений 30 травня 2022 року, набрав чинності 23 червня 2022 року та застосовується з 24 вересня 2023 року. «У регламенті встановлено: умови повторного використання певних захищених даних, що зберігаються органами державного сектору; правила для компаній, що надають послуги посередництва в передачі даних; основа для альтруїзму даних (добровільний обмін даними без винагороди); рамки для Європейської ради з інновацій у сфері даних (EDIB); заходи, що дозволяють безпечний потік неперсональних даних за межі ЄС» [243].

В даному напрямку є потреба національним законодавством: сформувати комплексне правове регулювання повторного використання захищених даних державного сектору, включаючи медичні дані; визначити компетентні органи, відповідальні за відповідні механізми управління та повторного використання даних; врегулювати діяльність посередників даних за моделлю DGA та встановити вимоги до їх незалежності й надійності; запровадити правовий механізм альтруїзму даних, зокрема можливість добровільного надання медичних даних для наукових та суспільно корисних цілей; забезпечити інтероперабельність української інфраструктури даних із європейськими просторами даних, особливо з EHDS; узгодити ці механізми із законодавством про захист персональних даних, кібербезпеку та EHDS.

На надмірному регулюванні наголошували Lukas von Ditfurth (Лукас фон Дітфурт), Gregor Lienemann (Грегор Лінеман) [274], які ставлять під сумнів доцільність настільки жорсткого регулювання нового ринку, який на момент прийняття DGA ще перебував на ранній стадії, адже надмірні обмеження можуть знижувати рівень активності інноваційного розвитку. Суперечність між цілями DGA та вимогами до посередників досліджувалися в праці Габріеле Каровано (Gabriele Carovano), Michèle Finck (Мішель Фінк) [115] в якій автори виявляють внутрішню суперечність щодо того, що DGA хоче стимулювати обмін даними, але одночасно встановлює такі вимоги до посередників, які можуть зробити деякі бізнес-моделі економічно нежиттєздатними. Беатріс Естевес (Beatriz Esteves), Віктор Родрігес Донсель (Víctor Rodríguez Doncel), Харшвардхан Дж. Пандіт (Harshvardhan J. Pandit), Дейв Льюїс (Dave Lewis) [147] показують складність практичної реалізації вимог DGA щодо data altruism, документації, політик та машинно-читаних правил, що свідчить про значну технічну й організаційну складність реалізації моделі. Гайко Ріхтер (Heiko Richter) [249] вказує, що DGA впливає на стимули для data intermediaries, конкуренцію та інновації, також автор наголошує на необхідності інтегрувати DGA в ширшу систему європейського регулювання обміну даними.

6. Регламент (ЄС) 2023/2854 про правила доступу до даних (Data Act) (Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)) [244]. Регламент ухвалений 13 грудня 2023 року, набрав чинності 11 січня 2024 року, а основні його положення застосовуються з 12 вересня 2025 року. Даним актом встановлено горизонтальні правила отримання доступу до даних, створених підключеними пристроями та пов’язаними послугами, порядок передачі даних та умови їх використання.

Ключовими положеннями є наступні: право користувача на дані, створені підключеними пристроями (статті 3 та 4); порядок передачі даних третій стороні за вибором користувача (статті 5 та 6); особливості доступу держави до даних у разі виняткової потреби (статті 14-22); мобільність даних і хмарних сервісів (статті 23-31); інтероперабельність даних (Стаття 33). Щодо впровадження даного документу в Україні на сьогодні створені лише передумови, а мови про початок впровадження йти не може, адже на сьогодні є значні досягнення в технологічній сфері, проте правові положення ще не відповідають технологічним рішенням, які вже впроваджені, зокрема: створено розвинену систему державних електронних інформаційних ресурсів та електронної взаємодії; Україна бере участь у програмі ЄС «Цифрова Європа» (2021–2027), через ратифікацію відповідної Угоди (Закон України № 2926-IX [53]).

Моріц Хеннеманн (Moritz Hennemann), Гордіан Ебнер (Gordian Ebner), Бенедикт Карстен (Benedikt Karsten) [217] критично аналізують архітектуру Data Act та вказують на значну кількість невизначених правових понять, складність взаємодії окремих положень та необхідність додаткового тлумачення. Азхар Рана (Rana Azhar) [82] вказує на потенційну напругу між прагненням Data Act розширити доступ до даних і обмеженнями GDPR. В статті Марі Вінродер (Marie Wienroeder) [217] аналізуються положення щодо доступу до даних, договорів та прав користувачів, в результаті чого авторка ставить питання, наскільки нові права користувачів будуть реально здійсненними, якщо технічна архітектура та договірні відносини залишаються складними. Моріц Хеннеманн (Moritz Hennemann), Гордіан Ебнер (Gordian Ebner), Бенедикт Карстен (Benedikt Karsten) [217] наголошують, що значне втручання законодавця у договірні відносини може створити додаткову правову невизначеність та compliance-витрати. Марія Белен Олмос Джуппоні (Maria Belén Olmos Giupponi), Ганнес Гофмейстер (Hannes Hofmeister) [227]

критично оцінюють вплив Data Act на структуру data economy, зокрема на стимули компаній інвестувати у створення та контроль даних, адже надмірне регулювання може змінити економічні стимули та бізнес-моделі.

В той же час завданнями для держави в контексті відповідності даному регламенту мають стати наступні:

1) закріплення права користувачів на доступ до даних, що створенні підключеними пристроями;

2) врегулювання передачі таких даних третім особам;

3) встановлення правил доступу державних органів;

4) запровадження європейських вимог до переходу між постачальниками хмарних та інших послуг обробки даних;

5) гармонізація вимог до інтероперабельності даних та цифрових платформ.

Нормативно-правові акти, які стосуються ***регулювання кібербезпеки цифрової трансформації системи охорони здоров'я,*** будуть розглянуті в наступних дослідженнях.

Багато уваги в системі нормативно-правового регулювання ЄС приділено питанням ***цифрової трансформації в медицині***. Зокрема, даному питанню присвячено два регламенти: Регламент (ЄС) 2017/745 про медичні вироби (MDR) та Регламент (ЄС) 2017/746 про медичні вироби для діагностики in vitro (IVDR). Зазначені регламенти формують базовий рівень захисту пацієнтів, встановлюючи єдині вимоги до безпечності, ефективності, клінічної оцінки, простежуваності та нагляду за медичними виробами й діагностичними тестами. Регламент (ЄС) 2017/745 про медичні вироби (MDR) прямо вимагає, щоб вироби не створювали неприйнятного ризику для пацієнтів, користувачів та інших осіб, а система ринкового нагляду дає можливість своєчасно виявляти та усувати небезпечні вироби. Регламент (ЄС) 2017/746 про медичні вироби для діагностики in vitro (IVDR), своєю чергою,

посилює безпеку діагностики, оскільки достовірність результатів IVD безпосередньо впливає на правильність діагностики та подальших медичних рішень. У сукупності ці регламенти забезпечують превентивну модель безпеки, за якої ризики мають виявлятися та мінімізуватися ще до і протягом використання технології, а не лише після виникнення шкоди. Більш детально зміст та критичні положення даних регламентів вивчено в контексті забезпечення безпеки в наступних дослідженнях.

До ***регламентів ЄС, які регулюють цифрові послуги*** відносяться:

1. *Регламент (ЄС) 2022/2065 про єдиний ринок цифрових послуг* (Digital Services Act) (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)) [242], який встановлює єдині правила для цифрових послуг у ЄС, зокрема щодо онлайн-платформ, прозорості, захисту користувачів, управління ризиками та відповідальності постачальників цифрових сервісів. Значення Регламенту для цифрової системи охорони здоров’я є опосередкованим, зокрема через регулювання цифрових платформ і онлайн-послуг, за допомогою яких можуть надаватися медичні послуги, поширюватися медична інформація або взаємодіяти пацієнти, медичні працівники та постачальники послуг. Ключовими положеннями Регламенту є:

- посилення права користувачів цифрових сервісів та встановлення вимог до прозорості діяльності платформ, що має значення для платформ, через які пацієнти можуть отримувати інформацію про здоров'я, взаємодіяти з медичними установами або користуватися цифровими медичними сервісами (статті 14, 16, 17, 20);
- визначення вимог до прозорості рекомендаційних систем та алгоритмів, які визначають, який контент бачить користувач, адже алгоритмічні системи можуть впливати на те, яку медичну інформацію отримує користувач (статті 27 та 28);

- встановлення додаткових обмежень щодо використання персональних даних для таргетованої реклами, зокрема заборона рекламувати на основі профілювання, якщо для цього використовуються спеціальні категорії персональних даних (стаття 26);

- формування системи нагляду за цифровими послугами через національних координаторів цифрових послуг, Європейську комісію та інші механізми контролю (статті 49, 56, 67-74).

- встановлення механізму оцінки та зменшення системних ризиків (статті 34 та 35).

Щодо критичних положень даного регламенту вони представлені в працях наступних вчених:

- Дженніфер Орландо-Селлінг (Jennifer Orlando-Salling) [229] критикує припущення, що DSA автоматично забезпечить однаковий рівень цифрових прав у всьому ЄС, адже існує нерівна спроможність держав-членів забезпечувати виконання Регламенту. Держави з недостатньо фінансованими та перевантаженими регуляторами можуть фактично забезпечувати значно слабший захист прав громадян, а це призводить до того що формальна гармонізація законодавства не гарантує фактичної гармонізації прав.

- Марселла Ацорі (Marcella Atzori) [101] вказує, що «Регламент про цифрові послуги (DSA) встановлює нову модель управління цифровою сферою в Європейському Союзі з метою боротьби з поширенням незаконного контенту та дезінформації, встановлення більш суворої відповідальності для цифрових платформ та гармонізації законодавства в ЄС. Однак Регламент викликав різку критику з боку громадянського суспільства та наукових кіл через його потенційний негативний вплив на основні права користувачів, зокрема на свободу слова» [101]. Крім того, авторка вказує на наступні проблеми: нечіткість і надмірна широта

окремих правових понять; надмірні або нереалістичні вимоги до платформ; значна роль державних органів у регулюванні цифрового контенту; ризик обмеження свободи вираження поглядів; потенційне зіткнення механізмів боротьби з дезінформацією з фундаментальними правами.

- Брам Дуйвенворде (Bram Duivenvoorde) та Каталіна Гоанта (Catalina Goanta) [139] вказують, що «Отриманий регуляторний вибір розмежування рекламних практик у соціальних мережах є щонайменше дивним, оскільки він не враховує характеристики цих практик або суттєву роль платформ соціальних мереж в інших формах реклами, окрім персоналізованої реклами. У статті критично розкривається три основні недоліки, пов'язані зі способом, у який Закон про цифрову рекламу (DSA) вирішує проблеми захисту прав споживачів у зв'язку з вибраними розробками цифрової реклами: узгодженість/фрагментація; незначні переваги для споживачів; та обмежена перспективність» [139].

На сьогодні в Україні даний регламент не імплементований в повному обсязі, хоча спроби відповідності його положень зроблені, зокрема через: прийняття Закону України «Про цифровий контент та цифрові послуги» [58]; трансформація інституційного забезпечення, що здійснюється Міністерством цифрової трансформації, Національною комісією, що здійснює державне регулювання у сфері електронних комунікацій, та інші органи, компетенція яких охоплює окремі аспекти цифрового середовища.

В той же час сукупність завдань залишається невирішеною, зокрема: гармонізація правил діяльності цифрових платформ із європейськими вимогами щодо прозорості, відповідальності та захисту користувачів; запровадження комплексного механізму регулювання незаконного цифрового контенту; посилення прозорості алгоритмів та рекомендаційних систем; забезпечення додаткового захисту від

використання даних про здоров'я для профілювання та таргетованої реклами; створення механізмів оцінки системних ризиків цифрових платформ; визначення компетентних органів, відповідальних за нагляд за цифровими послугами.

2. Регламент (ЄС) 2022/1925 про конкурентні та чесні ринки в цифровому секторі (Digital Markets Act) Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [241] встановлює спеціальні правила для великих цифрових платформ, які мають значний вплив на цифрові ринки. Регламент не є спеціальним актом у сфері охорони здоров’я, а його значення для цифрової трансформації системи охорони здоров’я є переважно структурним, адже регулює середовище, у якому функціонують великі цифрові платформи, операційні системи, магазини застосунків, пошукові системи та інші базові цифрові послуги.

Сферами регуляторного впливу регламенту є: забезпечення конкуренції на цифровому ринку; заборона використання даних бізнес-користувачів на користь самої платформи; забезпечення можливості взаємодії та доступу до платформ; обмеження поєднання персональних даних; захист інноваційних цифрових компаній.

Варто зазначити, що даний регламент неодноразово піддавався критиці з боку європейських вчених. Так, професорка права Університету Лідса Akman P. у 2022 році оприлюднила дослідження з критикою даного регламенту [88]. Критика стосувалася невідповідності регламенту конкурентному праву. Зокрема, Akman P. вказує, що регламент створює спеціальний режим регулювання для певних видів платформ без традиційного повного конкурентного аналізу кожної конкретної поведінки.

Орельєн Портуезе (Aurelien Portuese) [234] аналізуючи регламент зробив наступні висновки, що характеризують критичні положення:

«- закон про цифрові ринки (DMA) довільно розрізняє цифрові та нецифрові ринки, хоча цифрове розповсюдження є лише одним із багатьох способів, за допомогою яких компанії досягають кінцевих користувачів. Він повинен оцінювати конкуренцію всебічно, а не дискримінувати;

- туманна концепція цифрового «привратника» в DMA закріплює великі цифрові фірми та відбиває у них бажання впроваджувати інновації для конкуренції, а також створює пороговий ефект для малих та середніх фірм, оскільки це стримує успішне розширення;

- це являє собою зміну парадигми від ex post антимонопольного правозастосування до ex ante дотримання нормативних вимог - хоча й для вузько відібраного кола компаній - та фундаментальну перемогу принципу обережності над інноваціями;

- спотворюючи стимули для інновацій замість того, щоб посилювати їх, модель «превентивного антимонопольного регулювання» DMA загрожує життєздатності, динамізму та конкурентній справедливості європейської економіки на шкоду споживачам та фірмам усіх розмірів;

- з огляду на його фундаментальні недоліки, DMA може бути покращений лише частково. Першими кроками мають бути вирівнювання умов гри за допомогою реформ, які стосуються всіх фірм, а не лише «цифрових» ринків, та усунення розпливчастої концепції «контролера»;

- органи, відповідальні за правила ринкових розслідувань, повинні бути відокремлені від антимонопольних органів; їм потрібні рекомендації та можливості для встановлення фактів на основі доказів; і вони повинні динамічно аналізувати питання конкуренції, зосереджуючись на довгостроковій перспективі» [234].

Україна не застосовує Регламент (ЄС) 2022/1925 безпосередньо. Водночас Україна має розвинене конкурентне законодавство, яке створює загальну правову основу для протидії зловживанню ринковою владою та антиконкурентним практикам. Ключовим органом є Антимонопольний комітет України, який здійснює державний контроль за дотриманням законодавства про захист економічної конкуренції. Для цифрового сектору вже сформовані передумови для подальшого розвитку конкурентного регулювання цифрових ринків. Відповідно при формуванні державної політики цифрової трансформації Україна має врахувати визначені недоліки та гармонізувати національне законодавство зважаючи на критичні моменти.

Таким чином, в результаті проведеного дослідження, встановлено, що Європейський Союз 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 Європейському Союзі 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. Результатом цієї еволюції є цілісна система

нормативно-правових актів, 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.

4.2. Регулювання безпеки процесу цифрової трансформації системи охорони здоров'я в Європейському Союзі

Питання безпеки цифрової трансформації та безпеки функціонування системи охорони здоров'я є вкрай важливим питанням та досить врегульованим в Європейському Союзі. Безпеку варто розглядати як з позиції цифрової трансформації медицини так і з позиції забезпечення безпеки цифрової системи охорони здоров'я, зокрема кібербезпеки. При формуванні механізмів державного управління цифровою трансформацією системи охорони здоров'я в Україні необхідно враховувати євроінтеграційні вимоги та приділити особливу увагу безпеці. Адже вступ України до Європейського Союзу, визначає потребу інтеграції національної системи охорони здоров'я в європейський медичний простір для забезпечення транснаціональної медичної допомоги. В Європейському Союзі розроблено та впроваджено сукупність Регламентів, які регулюють питання безпеки медичного обладнання та безпеки цифрової системи охорони здоров'я в цілому. Відповідно актуалізується питання політико-правового аналізу даних регламентів для визначення їх критичних положень та відповідності національного законодавства.

Зазначені питання викладені в наукових 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), Джонатан Стокс (Jonathan Stokes), 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), 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.

В працях вчених розкриті особливості формування та реалізації регламентів ЄС щодо цифровізації системи охорони здоров’я, вагоме значення мають їх результати щодо забезпечення безпеки. Для України є вкрай важливим сьогодні вивчити питання безпекового характеру цифрової трансформації системи охорони здоров’я, що є можливим через правовий аналіз регламентів ЄС, які регулюють безпеку медичних виробів та кібербезпеку систем охорони здоров’я.

1. Безпека медичних виробів.

У контексті європейської інтеграції України особливого значення набуває вивчення нормативно-правових засад цифрової трансформації системи охорони здоров’я Європейського Союзу. Європейська інтеграція України, юридично закріплена Угодою про асоціацію та підтверджена наданням статусу країни-кандидата, зумовлює необхідність поступової адаптації національного законодавства до acquis communautaire, у тому числі у сфері обігу медичних виробів. Європейські регламенти у цій сфері визначають не лише технологічні та організаційні вимоги, а й формують комплексну систему безпеки медичних даних, цифрових технологій, медичних виробів та прав пацієнтів. Їх дослідження є важливим для визначення напрямів адаптації українського законодавства до права ЄС та забезпечення його сумісності з європейським цифровим простором. Водночас аналіз положень цих актів і наукової критики їх практичної реалізації дозволяє визначити потенційні ризики, регуляторні прогалини та інституційні виклики, які необхідно врахувати під час формування української моделі цифрової охорони здоров’я.

Регламенти (ЄС) 2017/745 (MDR) та (ЄС) 2017/746 (IVDR) є нині базовими актами, що визначають вимоги до безпеки, якості та клінічної ефективності медичних виробів і засобів діагностики in vitro на внутрішньому ринку ЄС, а тому становлять безпосередній орієнтир для реформування українського регуляторного середовища. Безпекова складова цих документів має подвійний вимір: з одного боку, вони спрямовані на захист життя і здоров'я пацієнтів через посилення клінічних доказів, відстежуваність виробів і постмаркетинговий нагляд, з іншого – формують стійкість системи охорони здоров'я до дефіциту критично важливих виробів, що в умовах воєнного стану та підвищеного навантаження на медичну інфраструктуру набуває для України значення питання національної безпеки.

Регламент (ЄС) 2017/745 про медичні вироби (MDR) (Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC) [239]. Даний документ був затверджений у 2017 році, а повноцінної сили набрав з 26 травня 2021 року. При затвердженні даного регламенту Європейський Союз переслідував мету підвищення безпеки пацієнтів, посилення вимог до якості та прозорості ринку після серії гучних скандалів з неякісними медичними імплантатами в ЄС, шляхом заміни попередніх Directives 93/42/EEC (MDD) та 90/385/EEC (AIMDD).

«Європейський Союз (ЄС) опублікував Регламент щодо медичних виробів (MDR) у квітні 2017 року для гармонізації процесу регуляторного розгляду та затвердження медичних виробів у всіх державах-членах ЄС. Вимоги MDR стали застосовуватися до всіх медичних виробів, що продаються в ЄС, у травні 2021 року. Це обов'язкова вимога для підприємств, які бажають продавати свої медичні вироби в ЄС, який є одним із найбільших ринків медичних виробів у світі. Вартість ринку у 2022 році оцінювалася приблизно в 150 мільярдів євро, а до 2027 року очікується, що вона досягне 170 мільярдів євро. Складність розробки нових та вдосконалених медичних виробів робить процес регуляторного затвердження складним для багатьох виробників виробів. Суворі вимоги, закладені в MDR, додають складності. Навіть виробники медичних виробів, раніше схвалених відповідно до MDD або AIMDD, не звільняються від вимог MDR. Застарілі пристрої, що все ще продаються на ринку, повинні бути повторно сертифіковані відповідно до положень MDR» [265].

Особливістю регламенту є те, що його дія охоплює, як власне медичне обладнання, так і програмне забезпечення, яке за своїм призначенням є медичним виробом. Регламентом передбачено сукупність нововведень, які стосуються:

- посилення вимог до клінічних доказів, що передбачає зобов'язання виробників надавати суттєво більше клінічних доказів, які були зібрані під час випробувань. «Європейський регламент щодо медичних виробів (EU MDR 2017/745) докорінно змінив спосіб, у який виробники медичних виробів демонструють відповідність вимогам. Окрім отримання маркування CE, від виробників очікується ведення повної технічної документації, створення надійних клінічних доказів та постійний моніторинг ефективності виробів протягом усього життєвого циклу продукту. Оскільки нормативні вимоги та контроль з боку нотифікованого органу продовжують розвиватися, структурований підхід до дотримання вимог ЄС MDR є надзвичайно важливим … Від сучасних виробників очікується ведення документації, яка є: повний та послідовний у всьому технічному файлі; підтверджено сучасними клінічними доказами; постійно оновлюється протягом усього життєвого циклу пристрою; відстежується в усіх супровідних документах; готовий до перевірки уповноваженим органом у будь-який час. Структурований контрольний список допомагає регуляторним командам виявляти прогалини в документації на ранній стадії, визначати пріоритети заходів щодо усунення недоліків та ефективніше готуватися до подання документів до регуляторних органів та наглядових аудитів» [151].

- забезпечення прозорості та відстежуваності, що передбачає потребу в маркуванні унікальним кодом для відстеження по всьому ланцюгу постачання. Відповідно створена єдина європейська база медичних виробів, де публікуються дані про реєстрацію виробів, сертифікати, клінічні дослідження та інциденти.

- здійснення безперервного постмаркетингового нагляду, що забезпечує контроль безпеки не лише до отримання маркування, адже виробників зобов’язують вести регулярний нагляд та подавати регулярні звіти безпеки.

- посилення кадрових вимог до суб’єктів ринку. Виробники та уповноважені представники зобов'язані мати у штаті кваліфіковану особу, відповідальну за регуляторну відповідність. В той же час органи з оцінки відповідності самі проходять жорсткіший аудит з боку регуляторів ЄС.

- запроваджено суворіші правила класифікації, через що багато виробів (особливо софт та багаторазовий хірургічний інструментарій) змінили клас на вищий та потребують залучення Нотифікованих органів.

Даний регламент як за змістом, так і за процесом реалізації неодноразово піддавався критиці, зокрема щодо:

- надмірного регуляторного навантаження та складність імплементації. Так, Сімоне Альбісінні (Simone Albisinni), Єнс Рассвайлер (Jens Rassweiler), Хендрік ван Поппель (Hendrik van Poppel) [89] звернули увагу на значні затримки сертифікації, недостатню спроможність системи оцінювання відповідності та ризик того, що медичні вироби не будуть доступні пацієнтам у необхідний момент;

- невідповідність регуляторної спроможності, адже Жак Катон (Jacques Caton), Ів Жюйєт (Yves Juillet) [116] виявили недостатню кількість та спроможність органів, які здійснюють оцінювання відповідності, та як наслідок ризик дефіциту медичних виробів.

- підвищення рівня ризику зменшення доступності медичних виробів. Посилення вимог до сертифікації може призводити до вилучення з ринку частини виробів, зокрема тих, які вже використовуються у клінічній практиці, що створює потенційний конфлікт між безпекою регулювання та доступністю медичної допомоги, на чому наголошували Сімоне Альбісінні (Simone Albisinni), Єнс Рассвайлер (Jens Rassweiler), Хендрік ван Поппель (Hendrik van Poppel) [89].

Україні доцільно гармонізувати вимоги до медичних виробів із MDR, одночасно спрощуючи та цифровізуючи процедури їх оцінки відповідності, особливо для інноваційних MedTech та малих і середніх підприємств. Водночас необхідно посилити інституційну спроможність органів державного нагляду, забезпечити достатню кількість компетентних органів оцінки відповідності та запровадити пропорційний ризик-орієнтований підхід, щоб підвищення безпеки не призводило до обмеження доступу пацієнтів до необхідних медичних виробів.

Регламент (ЄС) 2017/746 про медичні вироби для діагностики in vitro (IVDR) (Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance)) [213] є основним регуляторним документом Європейського Союзу, що визначає суворі вимоги до безпеки, якості та ефективності лабораторних та діагностичних тестів, реагентів і обладнання. Він набрав чинності у травні 2017 року та повністю застосовується з 26 травня 2022 року, повністю замінивши стару Директиву 98/79/EC (IVDD). Запровадження даного регламенту пов’язане із потребою забезпечення високого рівня захисту здоров'я пацієнтів і користувачів, гарантування точності та надійності діагностичних результатів, а також гармонізації ринку діагностичних засобів у ЄС. Ключовими нововведеннями є:

- заміна застарілої перелікової системи (List A, List B) на 4-рівневу систему класифікації на основі ризику для пацієнта та громадського здоров'я (від найнижчого до найвищого);

- орієнтовно 80–85 % усіх IVD-виробів (класи B, C, D) вимагають обов'язкового незалежного аудиту та залучення Нотифікованих органів;

- виробники повинні довести відповідність трьом складовим Performance Evaluation: наукова обґрунтованість (Scientific Validity); аналітична ефективність (Analytical Performance); клінічна ефективність (Clinical Performance).

- обов’язкове унікальне маркування кожного виробу та упаковки, публічна реєстрація виробів, сертифікатів, інцидентів та клінічних досліджень та обов’язковий систематичний збір реальних даних про роботу тестів після їх виходу на ринок.

Вченими [271], [272], [136] положення регламенту критикувалися в контексті: надмірного регуляторного навантаження на лабораторії; невизначеності поняття «еквівалентний тест»; гальмування інновацій у лабораторній медицині; недостатньої готовності регуляторної системи; недостатньої гнучкості для нових технологій.

У контексті цієї критики Україні варто гармонізувати систему регулювання IVD з IVDR, але не копіювати його механічно: необхідно забезпечити достатню спроможність органів оцінки відповідності, пропорційні вимоги для малих виробників та лабораторій і спеціальні механізми для in-house, orphan та інноваційних діагностичних тестів. Одночасно слід створити перехідні механізми та ризик-орієнтовану модель, щоб посилення контролю не спричинило дефіциту критично важливої діагностики.

Аналіз Регламентів (ЄС) 2017/745 (MDR) та (ЄС) 2017/746 (IVDR) дає підстави для кількох висновків прикладного характеру для України:

1) гармонізація національного регулювання обігу медичних виробів та засобів діагностики in vitro з цими актами є не факультативним вибором, а складовою євроінтеграційних зобов'язань України, водночас вона повинна здійснюватися шляхом адаптації, а не механічного копіювання: досвід ЄС засвідчив, що навіть держави з розвиненою регуляторною

інфраструктурою зіткнулися із затримками сертифікації, дефіцитом спроможності нотифікованих органів та ризиком вилучення з ринку виробів, які вже застосовувалися у клінічній практиці.

2) ключовим бар'єром є брак уповноважених органів з оцінки відповідності. Державі необхідно терміново посилити спроможність національних регуляторів, підготувати кваліфіковані кадри та розширити мережу акредитованих органів оцінювання, адже без цього формальне запозичення норм MDR/IVDR створить регуляторний бар'єр без відповідного приросту безпеки.

3) адаптація регуляторного поля має супроводжуватися максимальним спрощенням і цифровізацією процедур для вітчизняного MedTech-сектору, малих підприємств та лабораторних тестів власної розробки.

4) в умовах воєнного стану та підвищеного навантаження на систему охорони здоров'я безперебійний доступ до медичних виробів і критично важливої діагностики є питанням не лише захисту прав пацієнтів, а й національної безпеки, тому будь-яке посилення регуляторних вимог повинно супроводжуватися оцінкою впливу на доступність.

5) для уникнення регуляторного колапсу Україні критично необхідно передбачити чіткі перехідні періоди, аналогічні тим, які запровадив ЄС, надавши виробникам та медичним закладам час на адаптацію до нових вимог.

2. Кібербезпека цифрової трансформації системи охорони здоров'я.

У контексті повномасштабних цифрових загроз та євроінтеграційного поступу України напрям кібербезпеки цифрової трансформації системи охорони здоров'я набуває статусу фундаментальної складової національної безпеки. Цифрова трансформація системи охорони здоров'я, впровадження єдиних медичних реєстрів та

підключення критичної інфраструктури закладів охорони здоров’я до мережі роблять їх вразливими для кібератак, які можуть призвести не лише до витоку чутливих даних пацієнтів, а й до прямої загрози людському життю. Для України вивчення відповідного регуляторного досвіду Європейського Союзу є важливим з огляду на євроінтеграційні зобов’язання та необхідність підвищення стійкості національної системи охорони здоров’я до кіберзагроз.

Наступний блок актів формує кібербезпековий вимір права ЄС і охоплює три взаємодоповнювальні рівні регулювання:

- організаційно-інституційний (Директива (ЄС) 2022/2555 (NIS2), яка встановлює вимоги до кіберстійкості операторів критично важливих та важливих секторів, у тому числі охорони здоров’я);

- сертифікаційний (Регламент (ЄС) 2019/881 (Cybersecurity Act), що закріплює мандат ENISA та європейські схеми сертифікації кібербезпеки ІКТ-продуктів, послуг і процесів);

- продуктовий (Регламент (ЄС) 2024/2847 (Cyber Resilience Act), який запроваджує горизонтальні вимоги «безпеки за замовчуванням» до продуктів із цифровими елементами протягом усього життєвого циклу);

Для України їх дослідження має особливе значення: в умовах безпрецедентного тиску російських кібератак на державні реєстри, енергетичну та медичну інфраструктуру ці акти є одночасно і євроінтеграційним зобов'язанням, і практичним орієнтиром для побудови національної системи кіберзахисту. Їх аналіз дозволяє визначити основні безпекові стандарти, механізми управління кіберризиками та вимоги до кіберстійкості, які доцільно враховувати під час подальшої адаптації українського законодавства до права ЄС.

Директива (ЄС) 2022/2555 про заходи щодо забезпечення високого загального рівня кібербезпеки (NIS2) (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)) [135] є основоположним правовим актом Європейського Союзу, спрямованим на уніфікацію та посилення вимог кібербезпеки серед суб'єктів критичної інфраструктури та постачальників цифрових послуг. Вона офіційно замінила застарілу Директиву NIS1, ліквідувавши фрагментарність регулювання між державами-членами ЄС. Для системи охорони здоров’я NIS2 має безпосереднє значення, оскільки до сфери її дії включено сектор охорони здоров’я, зокрема заклади охорони здоров’я та виробників фармацевтичної продукції.

Ключовими нововведеннями Директиви (ЄС) 2022/2555, які стосуються цифрової трансформації системи охорони здоров’я, є наступними:

- вимоги до суб’єктів охорони здоров’я впроваджувати технічні, організаційні та операційні заходи для управління кіберризиками та мінімізації наслідків кіберінцидентів (стаття 21) та застосування ризик-орієнтованого та пропорційного підходів;

- забезпечення безперервності роботи цифрової інфраструктури (Стаття 21(2)) шляхом запровадження резервного копіювання, аварійного відновлення та кризового управління, що дозволить безперервно надавати медичні послуги у разі кібератаки чи іншого надзвичайного інциденту;

- забезпечення захисту цифрового ланцюга постачання (Статті 21(2)(d) та 21(3)) шляхом врахування кіберризиків, пов’язаних з постачальниками цифрових технологій та послуг, а також безпекою їхніх продуктів і процедур розроблення, що забезпечить безпеку закладів

охорони здоров’я, які використовують зовнішні інформаційні системи, хмарні сервіси та медичне програмне забезпечення;

- встановлює обов’язок повідомляти CSIRT або компетентний орган про значні кіберінциденти (Стаття 23), які істотно впливають на надання медичних послуг, що створює механізм оперативного реагування та накопичення інформації про кіберзагрози у сфері охорони здоров’я.

- забезпечення захисту персоналу закладів охорони здоров’я та контроль доступу (Стаття 21(2)), що передбачає заходи щодо кібергігієни, навчання персоналу, контролю доступу, управління активами, криптографії та багатофакторної автентифікації, для безпеки обробки великих обсягів чутливих персональних медичних даних.

- європейська координація кіберзахисту (Статті 10, 14–16), що передбачає функціонування компетентних органів, CSIRT, Групи співпраці та EU-CyCLONe для забезпечення обміну інформацією та координацію реагування на масштабні кіберкризи;

- сертифікація цифрових технологій на предмет кібербезпеки (Стаття 24), що передбачає можливість вимагати використання сертифікованих ІКТ-продуктів, послуг і процесів як додатковий механізм забезпечення довіри до цифрових технологій, що використовуються у критичних секторах, включаючи охорону здоров’я.

Фактично Директива (ЄС) 2022/2555 передбачає, що кібербезпека системи охорони здоров’я має забезпечуватися не на рівні окремих інформаційних систем, а бути комплексною системою. Безпека охоплює не тільки медичні дані, а й інфраструктуру, персонал, постачальників, програмне забезпечення, процеси відновлення та кризового управління.

Дональд Дейвід Стюарт Фергюсон (Donald David Stewart Ferguson) [155] вказує на обмеження Директиви. Зокрема, NIS2 може мати недостатню ефективність проти окремих типів кібератак, оскільки

передбачені нею заходи не охоплюють належним чином усі етапи життєвого циклу атаки, включаючи етапи розвідки. Так, автор робить наступний висновок: «під час аналізу моделі кібератак було виявлено, що перспектива інформаційної переваги є важливою на етапі розвідки кібератаки. Важливим та необхідним суб'єктам може бути надана значна допомога у виборі ефективних, відповідних та пропорційних заходів відповідно до вимоги управління ризиками та вимоги щодо впливу інциденту шляхом вжиття таких заходів під час розвідки: оцінка їхньої розвідувальної присутності, сканування вразливостей внутрішніх ресурсів, поглиблене тестування на проникнення, огляд внутрішньої та зовнішньої розвідки про загрози, а також моделювання загроз. Ці заходи не є прямо вимогою вимоги щодо управління ризиками або вимоги щодо впливу інциденту, і рекомендується враховувати ці заходи в наступних імплементаційних актах Директиви NIS 2» [155]. Сандра Шміц-Берндт (Sandra Schmitz-Berndt) [253] критично аналізує невизначеність критеріїв, за яких кіберінцидент підлягає обов’язковому повідомленню. Авторка зазначає, що нечіткі правові вимоги ускладнюють дотримання законодавства суб’єктами. Валентин Фогель (Valentin Vogel), Ніколас Зіглер (Nicolas Ziegler) [270] досліджують проблеми визначення критичності та сфери охоплення регулювання при переході від німецької моделі до NIS2, в той же час автори вказують на проблему складності визначення суб’єктів, що підпадають під посилені вимоги. Конрад Салек (Konrad Sałek), Патрик Файдек (Patryk Fajdek) [252] показали значні відмінності у транспозиції та практичній імплементації NIS2 у Франції, Німеччині та Польщі та відзначили проблеми інституційної готовності, фрагментації та визначення механізмів нагляду й забезпечення виконання.

Для України доцільно гармонізувати національні вимоги кібербезпеки у сфері охорони здоров’я з NIS2, посилюючи ризик-

орієнтоване управління, обов’язкове повідомлення про інциденти, безперервність роботи медичних систем та безпеку ланцюгів постачання. Водночас важливо не допустити механічного перенесення європейських вимог: необхідно врахувати обмежену інституційну та фінансову спроможність українських закладів охорони здоров’я, забезпечивши пропорційність вимог, централізовану підтримку кіберзахисту та чіткий розподіл повноважень між суб’єктами системи.

Регламент (ЄС) 2019/881 про Агентство ЄС з кібербезпеки та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій (Cybersecurity Act) (Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)) [240]. Документ ухвалено 17 квітня 2019 року, він набрав чинності 27 червня 2019 року та має пряму дію в усіх державах-членах. Ухвалюючи цей акт, Європейський Союз переслідував дві взаємопов'язані цілі: по-перше, інституційне посилення європейської архітектури кібербезпеки шляхом надання ENISA постійного (безстрокового) мандату замість попереднього обмеженого в часі, розширення її повноважень і ресурсів та перейменування на Агентство Європейського Союзу з кібербезпеки; по-друге, подолання фрагментації внутрішнього ринку, спричиненої існуванням паралельних національних схем сертифікації, через запровадження єдиної Європейської рамки сертифікації кібербезпеки (European Cybersecurity Certification Framework, ECCF).

Ключовими нововведеннями Регламенту є наступні:

- встановлення безстрокового мандату та розширення функцій ENISA (статті 1, 3, 4, 6, 7, 9, 10, 11, 12, 29-33, 34-37, 68), що охоплюють підтримку розроблення й імплементації політики ЄС, операційне співробітництво (у

тому числі участь у мережі CSIRT та підтримка держав-членів у реагуванні на масштабні інциденти), розвиток спроможностей, ситуаційну обізнаність, підготовку кадрів, а також провідну роль у підготовці схем сертифікації.

- створення європейської рамки сертифікації кібербезпеки (статті 8, 46, 47, 48, 49, 50, 51, 54), у межах якої ENISA на запит Європейської Комісії готує проєкти схем, що затверджуються імплементаційними актами Комісії та стають єдиними для всього внутрішнього ринку. Предметом сертифікації можуть бути не лише ІКТ-продукти, а й послуги та процеси.

- запровадження трьох рівнів гарантування безпеки («базовий», «істотний» та «високий») (статті 52, 53, 55), що визначають глибину та методи оцінювання відповідно до рівня ризику. Для базового рівня допускається самооцінювання виробником із видачею декларації відповідності ЄС, тоді як істотний і високий рівні вимагають залучення органів сертифікації.

- презумпційно добровільний характер сертифікації (статті 56 (2) та 56 (3)), якщо обов'язковість не встановлена іншим актом права ЄС або національним правом, із передбаченим періодичним оцінюванням доцільності переходу до обов'язкових схем.

- інституційне забезпечення та витіснення національних схем (статті 22, 57, 58, 59, 60, 62, 63, 64, 65) через створення національних органів сертифікації кібербезпеки, механізму взаємних експертних оцінок, Європейської групи з сертифікації кібербезпеки (ECCG) та Групи стейкхолдерів (SCCG).

Для України врахування цього досвіду має щонайменше чотири практичні виміри, зокрема:

- по-перше, доцільно розвивати національну систему оцінювання відповідності у сфері кібербезпеки на основі Common Criteria (ISO/IEC 15408) та ISO/IEC 17065/17025, орієнтуючись на визнання результатів сертифікації за схемою EUCC, а не на побудову власної паралельної схеми, яка згодом однаково підлягала б витісненню європейською;

- по-друге, необхідно завчасно сформувати інституційну основу шляхом визначення національного органу сертифікації кібербезпеки для забезпечення акредитації лабораторій та органів оцінювання відповідності та підготовки експертного кадрового складу;

- по-третє, з огляду на критику добровільної моделі та з урахуванням безпекових реалій України, обґрунтованим є ризик-орієнтований підхід із обов'язковою сертифікацією для чітко визначеного кола об'єктів.

Регламент (ЄС) 2024/2847 про горизонтальні вимоги до кібербезпеки продуктів з цифровими елементами (Cyber Resilience Act) (Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)) [247]. Регламент ухвалено 23 жовтня 2024 року, він набрав чинності 10 грудня 2024 року, однак застосовується поетапно: положення щодо нотифікації органів оцінки відповідності - з 11 червня 2026 року, обов'язки щодо повідомлення про активно експлуатовані уразливості та серйозні інциденти - з 11 вересня 2026 року, а решта вимог, включно з обов'язковим маркуванням CE, - з 11 грудня 2027 року (ст. 71). Даний акт вперше запровадив горизонтальні вимоги до кібербезпеки для всіх продуктів із цифровими елементами, які розміщуються на внутрішньому ринку. Мета полягала в усуненні двох системних недоліків, зафіксованих у преамбулі:

- низького рівня кібербезпеки продуктів, у тому числі через недостатність і несвоєчасність оновлень безпеки;

- неможливості для користувачів оцінити рівень захищеності продукту перед його придбанням.

- заповнює прогалину між сертифікацією (Cybersecurity Act), яка є переважно добровільною, та вимогами до операторів критично важливих секторів (NIS2), які не охоплюють самі продукти.

Даний регламент містить положення, які:

- встановлюють обов'язок виробників забезпечувати кібербезпеку продуктів із цифровими елементами вже на етапах проєктування, розроблення та виробництва, а також проводити оцінювання кіберризиків протягом життєвого циклу продукту (статті 6 та 13);

- передбачають обов'язки виробника щодо виявлення, усунення та повідомлення про вразливості, а також забезпечення безпеки продукту протягом періоду його підтримки, особливо для цифрових медичних технологій, які можуть залишатися в експлуатації багато років (стаття 13 та частина II Додатка I);

- визначають, що продукти повинні розроблятися таким чином, щоб забезпечувати належний рівень кібербезпеки за замовчуванням, зокрема щодо захисту від несанкціонованого доступу, використання криптографії, безпечних налаштувань та мінімізації потенційних вразливостей (стаття 13);

- виділяють «важливі продукти з цифровими елементами», для яких встановлюються спеціальні процедури оцінки відповідності, зокрема до таких категорій належать продукти, кіберкомпрометація яких може створити значний ризик для здоров'я, безпеки користувачів або інших систем (стаття 7);

- встановлюють спеціальні вимоги щодо повідомлення про активно експлуатовані вразливості та серйозні інциденти, пов'язані з безпекою продуктів;

Так, Регламент встановлює горизонтальні вимоги до кібербезпеки широкого кола цифрових продуктів, які можуть використовуватися в охороні здоров'я, однак безпосередньо медичні вироби та IVD регулюються Регламентом (ЄС) 2017/745 про медичні вироби (MDR) та Регламентом (ЄС) 2017/746 про медичні вироби для діагностики in vitro.

Тому для цифрової медицини CRA важливий насамперед у частині захисту цифрових компонентів, програмного забезпечення та інших продуктів, що не підпадають під спеціальне медичне регулювання.

Відповідно в Україні необхідно прийняти національний технічний регламент кібербезпеки продуктів з цифровими елементами на основі CRA, а вітчизняні компанії повинні запровадити процедури оцінки ризиків кібербезпеки та автоматичного оновлення програмного забезпечення ще на етапі розробки. Також є потреба у створенні акредитованих випробувальних лабораторій для оцінки кіберстійкості цифрових продуктів за вимогами CRA. Це допоможе інтегрувати національну систему сертифікації до рамок ЄС, що забезпечить вільний експорт українських високотехнологічних продуктів на європейський ринок.

Забезпечення безпеки цифрової трансформації системи охорони здоров’я має двоєдину природу і охоплює безпеку медичних виробів (зокрема MedTech та спеціалізованого ПЗ) та кібербезпеку цифрової інфраструктури. У контексті євроінтеграції України ключовим завданням є адаптація національного законодавства до ключових нормативно-правових актів Європейського Союзу. Для України адаптація відповідних підходів є важливою складовою європейської інтеграції та формування кіберстійкої цифрової системи охорони здоров’я. Водночас їх імплементація має здійснюватися з урахуванням національної інституційної спроможності, ресурсних можливостей медичних закладів та специфіки воєнних кіберзагроз.

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.

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.

4.3. Особливості державного управління цифровою трансформацією в країнах-членах Європейського Союзу

Адаптація національного законодавства в сфері цифрової трансформації охорони здоров'я до вимог Європейського Союзу відбувалася в кожній країні по-різному, зважаючи на сукупність факторів соціально-економічного, політико-правового та культурно-ментального характеру. Відповідно єдиного правильного варіанту євроінтеграційних процесівпроцесів не існує, і тому кожна країна обрала власну стратегію цифрової трансформації у відповідності до вимог Європейського Союзу.

«В Україні, де процес цифрової трансформації розгортається на тлі затяжної гібридної війни, системних реформ в системі охорони здоров'я, обмеженості ресурсів та високого рівня соціальної вразливості проблема набуває особливої гостроти. В умовах воєнного стану публічна політика постає перед завданням як забезпечення безперервного функціонування критичної інфраструктури, так і налагодження ефективних каналів комунікації, запобігання інформаційним загрозам, формування довіри до цифрових інструментів та державних рішень, які ухвалюються та реалізуються в умовах невизначеності. Окремої уваги потребує аспект міжінституційної та міжсекторної взаємодії в реалізації цифрової політики в системі охорони здоров'я. Сучасна модель публічного управління передбачає активну участь приватного сектору, громадянського суспільства та наукових установ у формуванні, реалізації та оцінюванні політики, однак в українських реаліях бракує системної координації цих процесів, що ускладнює досягнення узгоджених результатів. Крім того, недостатність інституціоналізованих механізмів антикризового реагування, дефіцит підготовлених фахівців у сфері цифрової етики, управління конфліктами та цифрової комунікації посилює вразливість

системи охорони здоров’я до зовнішніх і внутрішніх загроз. Країни ЄС демонструють ефективні моделі поєднання цифровізації з прозорим публічним управлінням, залученням громадськості до процесу прийняття рішень, розвитком комунікацій та запровадженням стандартів кібербезпеки. Аналіз цих моделей дозволяє виокремити дієві інструменти, які можуть бути адаптовані до українських реалій» [79].

Україна хоч і не є членом Європейського Союзу, знаходиться на цьому шляху і вже сьогодні має забезпечити відповідність цифрової трансформації системи охорони здоров’я вимогам ЄС для інтеграції в єдиний європейський медичних інформаційний простір. Це вимагає науково обґрунтованих державно-управлінських рішень, які мають базуватися на досвіді країн-членів ЄС, що показали значні успіхи в даному питанні.

«У 2025 році держави-члени досягли подальшого прогресу в досягненні цілі електронної охорони здоров’я, яка полягає в тому, щоб «100% громадян ЄС мали доступ до своїх електронних медичних карток до 2030 року». Сукупний показник електронної охорони здоров’я для ЄС-27 досяг середнього значення 87%, що на 4 відсоткові пункти більше, ніж у 2024 році. Усі держави-члени мають службу онлайн-доступу; чотири держави-члени керують регіональними службами (Ірландія, Італія, Іспанія та Швеція). Загалом, 18 держав-членів, Ісландія та Норвегія підвищили свій рівень зрілості порівняно з 2024 роком, що відображає такі покращення, як ширша доступність типів даних та більша кількість постачальників медичних послуг, які підключені та обмінюються даними. Дев'ять держав-членів зберегли той самий рівень зрілості, включаючи Бельгію та Естонію, які досягли 100% складеного показника зрілості у 2024 році. Досягнуто значного прогресу в покращенні доступності даних електронних медичних карток. Найбільш широко доступними є дані про ідентифікацію (100%),

персональну інформацію (98%), електронні виписки ліків (91%) та електронні рецепти (89%). Однак медичні зображення (35%) та медичні пристрої та імплантати (59%) залишаються менш доступними через технічні обмеження та фрагментовані системи» [263].

За 2025 Digital Decade eHealth Indicator Study (дані станом на 31 грудня 2024 р.) середній показник ЄС становив 83 %. Найвищі результати демонстрували країни Північної та Балтійської Європи, тоді як частина країн Центральної та Південної Європи суттєво відставала. Першими в рейтингу були наступні країни-члени ЄС: Бельгія, Данія, Естонія. Розглянемо особливості цифрової трансформації систем охорони здоров'я зазначених країн-членів Європейського Союзу (табл. 4.1).

Бельгія. Нормативне закріплення цифрової трансформації системи охорони здоров'я Бельгії відбулося у 2008 році із прийняттям Закону щодо створення та організації платформи електронної охорони здоров'я від 21 серпня 2008 року [192], що є базовим нормативним актом цифровізації охорони здоров'я Бельгії, яким створено eHealth-platform як державну установу та визначено її повноваження щодо електронного обміну медичною інформацією. Закон закріплює вимоги до інформаційної безпеки, захисту приватності, інтероперабельності, електронних медичних записів, управління доступом, шифрування та анонімізації медичних даних (статті 2, 4, 5).

В той же час, система державного регулювання цифрової трансформації системи охорони здоров'я в Бельгії безпосередньо пов'язана із імплементацією директив та регламентів Європейського Союзу, зокрема:

Таблиця 4.1

Державне управління процесами цифрової трансформації системи охорони здоров'я країн-членів ЄС

БЕЛЬГІЯ			
Система державного регулювання та імплементація Директив і Регламентів ЄС			
Директива (ЄС) 2022/2555 (NIS 2)	*Регламент (ЄС) 2016/679 (GDPR)*	*Регламент (ЄС) 2017/745 (MDR)*	*Регламент (ЄС) 2017/746 (IVDR)*
- Закон про створення рамок для кібербезпеки мереж та інформаційних систем загального інтересу для громадської безпеки від 26 квітня 2024 року [193] - Королівський указ про імплементацію Директиви NIS 2 [93]	- Закон про захист фізичних осіб стосовно обробки персональних даних [194]	- Закон щодо медичних виробів [196]; - Королівський указ про внесення змін та скасування різних положень, що стосуються медичних виробів від 21 квітня 2021 року [187]; - Королівський указ щодо клінічних досліджень медичних виробів від 18 травня 2021 року [96]	- Закон про медичні вироби для діагностики in vitro від 15 червня 2022 року [195]; - Королівський указ про впровадження закону про медичні вироби для діагностики in vitro [94]; - Королівський указ щодо досліджень ефективності медичних виробів для діагностики in vitro [95]
Регламент (ЄС) № 910/2014 (eIDAS)	*Регламент (ЄС) 2019/881 (Cybersecurity Act)*	*Регламент (ЄС) 2025/327 (EHDS)*	*Регламент (ЄС) 2024/1689 (AI Act)*
- Бельгійська eID-схема Belgian eID Scheme FAS / itsme® була офіційно нотифікована Європейській Комісії відповідно до eIDAS [146]	- положення реалізуються через участь Бельгії у європейській системі кіберсертифікації та діяльність Centre for Cybersecurity Belgium (CCB).	- Бельгія формує відповідну національну інституційну структуру, зокрема через Health Data Agency для вторинного використання медичних даних та eHealth-platform для первинного використання	- Бельгія формує національні механізми імплементації та компетентні органи відповідно до вимог AI Act.
Суб'єкти цифрової трансформації системи охорони здоров'я			
eHealth-platform [141]	*Федеральна державна служба охорони здоров'я, безпеки харчового ланцюга та довкілля [170]*	*Національний інститут страхування здоров'я та непрацездатності [180]*	*Бельгійське агентство даних охорони здоров'я [106]*
- федеральна державна установа, яка відповідає за стратегію eHealth, електронний обмін медичною інформацією, інтероперабельність, базові цифрові сервіси та забезпечення інформаційної безпеки й приватності	- федеральний орган політики у сфері охорони здоров'я, що формує та реалізує федеральну політику охорони здоров'я, у тому числі політики цифрової трансформації та взаємодії з іншими державними суб'єктами	- відповідає за значну частину цифрових процесів у системі обов'язкового медичного страхування, електронну взаємодію між медичними працівниками, пацієнтами та страховою системою	- забезпечує доступність медичних даних для досліджень, формування політики та інновацій, одночасно розвиваючи безпечні методи обміну даними та приділяючи особливу увагу кібербезпеці

Продовження табл. 4.1

Центр кібербезпеки Бельгії [118]	*Федеральне агентство з лікарських засобів та медичних виробів Бельгії [154]*	*Комітет з інформаційної безпеки [177]*
- національний орган Бельгії з кібербезпеки, що координує національну політику кібербезпеки, здійснює нагляд та координує реагування на кіберінциденти; він також відіграє центральну роль у реалізації NIS2	- компетентний федеральний орган щодо лікарських засобів і медичних виробів, що реалізує цифрову трансформацію в контексті MDR, IVDR та програмного забезпечення, яке є медичним виробом, а також для ринкового нагляду та безпеки відповідної продукції	- орган відіграє регуляторну та наглядову роль щодо захисту персональних медичних даних

ДАНІЯ			
Система державного регулювання			
Закон Данії № 1758 від 29 грудня 2025 року «Про цифрове здоров'я Danmark» [199]	*Закон Данії № 1760 від 29 грудня 2025 року «Про внесення змін до Закону про охорону здоров'я та низки інших законів» [200]*	*Консолідований Закон Данії про охорону здоров'я [104]*	*Наказ № 255 від 24 лютого 2022 року «Про функціонування спільної цифрової інфраструктури у сфері охорони здоров'я» [105]*
Імплементація Директив і Регламентів ЄС			
Директива (ЄС) 2022/2555 (NIS 2)	*Регламент (ЄС) 2016/679 (GDPR)*	*Регламент (ЄС) № 910/2014 (eIDAS)*	*Регламент (ЄС) 2022/868 (DGAct)*
- Закон про заходи щодо забезпечення високого рівня кібербезпеки від 1 липня 2025 року [206]	- Закон про додаткові положення до Регламенту щодо захисту фізичних осіб у зв'язку з обробкою персональних даних і щодо вільного руху таких даних [128]	- Закон про додаткові положення до Регламенту щодо електронної ідентифікації та довірчих послуг для електронних транзакцій на внутрішньому ринку [204]	- Закон про додаткові положення до Регламенту (ЄС) 2022/868 щодо європейського управління даними та про внесення змін до Регламенту (ЄС) 2018/1724 [202]
Регламент (ЄС) 2023/2854 (Data Act)	*Регламент (ЄС) 2019/881 (Cybersecurity Act)*	*Регламенти (ЄС) 2017/745 (MDR)*	*Регламенти (ЄС) 2017/746 (IVDR)*
- Закон про додаткові положення до Регламенту щодо гармонізованих правил справедливого доступу до даних та їх використання [198]	- Закон про додаткові положення до Регламенту щодо Агентства ЄС з кібербезпеки (ENISA), кібербезпекової сертифікації ІКТ [205]	- Консолідований закон Данії № 682 від 29 травня 2023 року про медичні вироби [103]	

Регламент (ЄС) 2022/2065 (Digital Services Act)	*Регламент (ЄС) 2022/1925 (Digital Markets Act)*	*Регламент (ЄС) 2024/1689 (AI Act)*
- Закон про забезпечення виконання Регламенту Європейського Парламенту і Ради про єдиний ринок цифрових послуг [201]	- Закон про додаткові положення до Регламенту Європейського Парламенту і Ради про цифрові ринки [197]	- Закон про додаткові положення до Регламенту про штучний інтелект [203]

Продовження табл. 4.1

Суб'єкти цифрової трансформації системи охорони здоров'я			
Регіони Данії (Danske Regioner) [127]	*Данське управління даними охорони здоров'я (Sundhedsdatastyrelsen) [260]*	*Цифрове здоров'я Данії (Digital Sundhed Danmark) [134]*	*Данська асоціація місцевих органів влади (KL) [191]*
- Забезпечують функціонування регіональної частини системи охорони здоров'я, включаючи лікарняні IT-системи, регіональну цифрову інфраструктуру та заходи з кібербезпеки, а також беруть участь в управлінні цифровою трансформацією	- центральний державний орган у сфері медичних даних і цифровізації охорони здоров'я, що розробляє та забезпечує функціонування національних цифрових рішень, реєстрів, стандартів та інфраструктури, а також бере участь у забезпеченні інформаційної безпеки сектору	- національна організація, яка об'єднає Данське управління даними охорони здоров'я, портал sundhed.dk, MedCom, Національний центр геному та низку спільних національних IT-завдань регіонів для забезпечення більш узгодженого розвитку цифрових рішень, інфраструктури та використання медичних даних	- представляє муніципалітети та бере участь у формуванні й реалізації спільної політики цифровізації охорони здоров'я, оскільки значна частина медичних і соціально-медичних послуг надається на муніципальному рівні.
Данський центр медичної комунікації (MedCom) [212]	*Національний центр геному Данії (Nationalt Genom Center) [218]*	*Міністерство внутрішніх справ та охорони здоров'я Данії*	*Національний портал охорони здоров'я Данії (sundhed.dk) [259]*
- забезпечує стандартизацію та електронний обмін медичною інформацією між лікарнями, лікарями, муніципалітетами та іншими учасниками системи охорони здоров'я	- забезпечує національну інфраструктуру геномних даних та розвиток персоналізованої медицини	- формує державну політику у сфері охорони здоров'я, визначає загальні напрями цифрової трансформації та здійснює політичне й нормативне управління сектором	- забезпечує громадянам і медичним працівникам доступ до цифрових медичних послуг та інформації та є одним із ключових елементів національної цифрової інфраструктури охорони здоров'я

Данське агентство цифрового уряду (Digitaliseringsstyrelsen) [125]	*Центр кібербезпеки Данії (Center for Cybersikkerhed, CFCS) [258]*	*Данський центр кібербезпеки сектору охорони здоров'я (SundCERT) [126]*
- центральний орган державної цифровізації, що відповідає за загальнодержавні цифрові рішення, цифрову ідентифікацію, електронні довірчі послуги та бере участь у реалізації європейського цифрового законодавства, що має значення і для охорони здоров'я	- національний центр кібербезпеки, який здійснює моніторинг кіберзагроз, аналізує загрози та забезпечує загальнодержавні функції у сфері кіберзахисту.	- спеціалізований секторний механізм кібербезпеки охорони здоров'я. Забезпечує моніторинг кіберзагроз, попередження суб'єктів сектору та підтримку під час кіберінцидентів

Продовження табл. 4.1

Децентралізований підрозділ кібер- та інформаційної безпеки сектору охорони здоров'я (DCISSund) [255]	*Центр аналізу безпеки (Security Analysis Center, SAC) [126]*	*Центр операційної безпеки (Security Operations Center, SOC) [126]*	
- забезпечує координацію кібербезпеки між суб'єктами сектору охорони здоров'я, організовує обмін інформацією про загрози та вразливості, попередження і підтримку суб'єктів під час інцидентів	- аналітичний компонент системи кібербезпеки охорони здоров'я, який здійснює збір та аналіз інформації про кіберзагрози і сприяє ранньому виявленню потенційних атак	- забезпечує оперативний моніторинг IT-середовища, виявлення кіберзагроз та реагування на інциденти у цифровій інфраструктурі сектору охорони здоров'я	
ЕСТОНІЯ			
Система державного регулювання			
Закон про організацію медичних послуг [173]	*Закон про захист персональних даних [233]*	*Закон про публічну інформацію [251]*	
Закон про електронні комунікації [142]	*Закон про кібербезпеку [123]*	*Закон про документи, що посвідчують особу [182]*	
Імплементація Директив і Регламентів ЄС			
Директива (ЄС) 2022/2555 (NIS2)	*Регламент (ЄС) 2016/679 (GDPR)*	*Регламент (ЄС) № 910/2014 (eIDAS)*	*Регламент (ЄС) 2022/868 (Data Governance Act)*
- Закон про кібербезпеку [123]	- Закон про захист персональних даних [233]	- Закон про електронну ідентифікацію та довірчі послуги для електронних транзакцій [145]	- Закон про публічну інформацію [251]
Регламент (ЄС) 2023/2854 (Data Act)	*Регламент (ЄС) 2024/1689 (AI Act)*	*Регламент (ЄС) 2017/746 (IVDR)*	*Регламент (ЄС) 2017/745 (MDR)*
- Концепції управління даними [91]	- державна програма розвитку та впровадження ШІ [168]	- Закон про медичні вироби [214]	
Суб'єкти цифрової трансформації системи охорони здоров'я			
Державна система інформації про здоров'я (Health Information System) [172]	*Державна інспекція із захисту даних (Andmekaitse Inspektsioon) [148]*	*Департамент здоров'я Естонії (Terviseamet) [171]*	*CERT-EE — група реагування на комп'ютерні інциденти Естонії [179]*
- національна база медичних даних, що забезпечує обмін інформацією між надавачами медичних послуг	- наглядає за дотриманням законодавства про захист персональних даних та GDPR, що має особливе значення для обробки медичних даних	- державний орган у сфері громадського здоров'я, що здійснює регуляторні та наглядові функції, у тому числі щодо медичних виробів	- функціонує в системі RIA та забезпечує приймання повідомлень, координацію реагування й обмін інформацією щодо кіберінцидентів

Продовження табл. 4.1

Міністерство соціальних справ Естонії [216]	*Центр інформаційних систем охорони здоров'я та соціального забезпечення (TEHIK) [169]*	*Державне агентство інформаційних систем (RIA) [250]*	*Естонський фонд медичного страхування (Tervisekassa) [262]*
- формує державну політику у сфері охорони здоров'я та визначає стратегічні напрями цифрової трансформації, а також є співконтролером національної Системи інформації про здоров'я	- IT-центр у сферах охорони здоров'я, соціального забезпечення та праці, що розробляє та адмініструє ключові цифрові рішення, зокрема Систему інформації про здоров'я та Портал здоров'я	- центральний орган у сфері державної інформаційної інфраструктури, цифрових сервісів та кібербезпеки; забезпечує, зокрема, функціонування X-Road та приймання повідомлень про кіберінциденти	- забезпечує функціонування системи медичного страхування та бере участь у розвитку цифрових медичних сервісів, а також разом із Міністерством соціальних справ є співконтролером Системи інформації про здоров'я

- Закон про створення рамок для кібербезпеки мереж та інформаційних систем загального інтересу для громадської безпеки від 26 квітня 2024 року [193] та Королівський указ про імплементацію Директиви NIS 2 [93] є національними нормативно-правовими документами Бельгії, які визначають імплементацію Директиви (ЄС) 2022/2555 (NIS2). Закон «спрямований на посилення кібербезпеки, управління інцидентами та наглядових заходів для суб'єктів, що надають послуги, необхідні для підтримки критично важливої соціальної чи економічної діяльності. Він також спрямований на покращення координації державної політики щодо кібербезпеки» [117].

- Закон про захист фізичних осіб стосовно обробки персональних даних [194] є бельгійським законом, який доповнює та забезпечує практичне застосування Регламенту (ЄС) 2016/679 (GDPR) у Бельгії, визначаючи національні правила захисту персональних даних, повноваження контролюючого органу та окремі винятки й спеціальні режими обробки даних;

- Закон щодо медичних виробів [196] встановлює національні правила, необхідні для практичного застосування Регламенту (ЄС) 2017/745 (MDR), зокрема визначає компетентним органом бельгійське FAMHP та встановлює національні механізми нагляду, контролю, клінічних досліджень і відповідальності у сфері медичних виробів;

- Королівський указ про внесення змін та скасування різних положень, що стосуються медичних виробів від 21 квітня 2021 року [187] є бельгійським підзаконним актом, прийнятий у зв’язку із застосуванням Регламенту (ЄС) 2017/745 (MDR), який адаптував і скасував окремі положення попереднього національного регулювання медичних виробів відповідно до нової системи ЄС, а також змінив національні правила щодо обігу та реєстрації медичних виробів, у тому числі скасував обов’язкову реєстрацію експортерів медичних виробів;

- Королівський указ щодо клінічних досліджень медичних виробів від 18 травня 2021 року [96] - бельгійський підзаконний акт, прийнятий для практичної реалізації вимог Регламенту (ЄС) 2017/745 (MDR) щодо проведення клінічних досліджень медичних виробів у Бельгії. Цей указ встановлює національні процедурні та організаційні правила проведення клінічних досліджень медичних виробів відповідно до Регламенту (ЄС) 2017/745 (MDR), зокрема визначає роль FAMHP та етичних комітетів і вимоги до оцінювання безпеки таких досліджень;

- Закон про медичні вироби для діагностики in vitro від 15 червня 2022 року [195] встановлює бельгійські національні заходи для застосування Регламенту (ЄС) 2017/746 (IVDR), зокрема визначає національні правила щодо нагляду, обігу та використання медичних виробів для діагностики in vitro;

- Королівський указ про впровадження закону від 15 червня 2022 року щодо медичних виробів для діагностики in vitro [94] конкретизує національні механізми застосування Регламенту (ЄС) 2017/746 (IVDR) та Закону від 15 червня 2022 року, зокрема визначає повноваження FAMHP/AFMPS, процедури реєстрації операторів, нагляду за ринком, повідомлення про серйозні інциденти та застосування обмежувальних заходів щодо небезпечних або невідповідних IVD;

- Королівський указ щодо досліджень ефективності медичних виробів для діагностики in vitro від 25 вересня 2022 року [95] встановлює національні правила проведення досліджень характеристик IVD, зокрема процедури їх авторизації та оцінювання, вимоги до досліджень із інвазивним забором зразків, companion diagnostics та IVD, що виробляються і використовуються безпосередньо закладами охорони здоров’я;

Бельгія сформувала цілісну правову та інституційну основу цифрової трансформації охорони здоров’я, у якій цифрова трансформація розглядається одночасно як інструмент підвищення якості медичної допомоги та як питання захисту інформації. Інституційна модель

характеризується розподілом повноважень: eHealth-platform забезпечує цифрову інфраструктуру та електронний обмін медичними даними, Health Data Agency координує вторинне використання медичних даних, а Centre for Cybersecurity Belgium (CCB) здійснює загальнодержавну координацію та нагляд у сфері кібербезпеки.

Бельгійська модель державного управління цифровою трансформацією системи охорони здоров'я поєднує централізоване встановлення стандартів і вимог безпеки з децентралізованим зберіганням та обміном медичними даними. Це забезпечує високий рівень інтероперабельності без необхідності концентрації всієї медичної інформації в єдиній базі. Для України найбільш цінним є даний підхід, що дозволить поєднати єдину державну цифрову архітектуру, чіткий розподіл інституційних повноважень, інтероперабельність та кібербезпеку як невід'ємну складову цифрової трансформації.

Данія. Ключовими нормативно-правовими актами цифрової трансформації системи охорони здоров'я Данії є:

- Закон Данії № 1758 від 29 грудня 2025 року «Про цифрове здоров'я Danmark» [199] передбачає створення цифрового здоров'я Данії як національної організації, відповідальної за координацію та розвиток цифрових рішень, цифрової інфраструктури й використання даних у системі охорони здоров'я. Закон є основою переходу Данії до більш інтегрованої моделі управління цифровою охороною здоров'я;

- Закон Данії № 1760 від 29 грудня 2025 року «Про внесення змін до Закону про охорону здоров'я та низки інших законів» [200] встановлює національні повноваження щодо планування цифровізації та управління даними у системі охорони здоров'я, а також нові правила функціонування спільної цифрової інфраструктури. Створює правові передумови для централізованої координації цифрових рішень у сфері охорони здоров'я;

- Консолідований Закон Данії про охорону здоров'я [104] є базовим законодавчим актом системи охорони здоров'я Данії та визначає правові засади використання медичних даних, електронних медичних записів і цифрової інфраструктури, а також надає правові підстави для встановлення вимог до IT-систем та цифрових рішень у сфері охорони здоров'я;

- Наказ № 255 від 24 лютого 2022 року «Про функціонування спільної цифрової інфраструктури у сфері охорони здоров'я» [105] регулює функціонування спільної цифрової інфраструктури охорони здоров'я, зокрема електронний обмін медичною інформацією, доступ до медичних даних та реєстрацію доступу до них, забезпечуючи практичну реалізацію цифрової взаємодії між учасниками системи охорони здоров'я.

Вагоме значення в системі правового забезпечення цифрової трансформації системи охорони здоров'я Данії мають нормативно-правові акти, які визначають їх відповідність Директивам та Регламентам Європейського Союзу, зокрема:

- Закон про заходи щодо забезпечення високого рівня кібербезпеки [206] передбачає імплементацію NIS2 та набрав чинності 1 липня 2025 року. Закон встановлює вимоги до управління кіберризиками, повідомлення про інциденти, реєстрації суб'єктів та відповідальності керівництва. Для сектору охорони здоров'я відповідальним секторним органом визначено Danish Health Data Authority (Sundhedsdatastyrelsen), яка здійснює консультування та нагляд за виконанням NIS2 щодо відповідних суб'єктів системи охорони здоров'я. Варто зазначити, що станом на 2025 рік Європейська Комісія зазначала, що Данія ще не повідомила про повну транспозицію NIS2, хоча національний NIS2 Act уже набув чинності [220].

- Закон про додаткові положення до Регламенту щодо захисту фізичних осіб у зв'язку з обробкою персональних даних і щодо вільного руху таких даних [128] є основним національним законом Данії, що доповнює та забезпечує застосування Регламенту (ЄС) 2016/679 (GDPR), встановлюючи національні правила обробки персональних даних, здійснення нагляду та відповідальності за порушення вимог щодо захисту даних;

- Закон про додаткові положення до Регламенту щодо електронної ідентифікації та довірчих послуг для електронних транзакцій на внутрішньому ринку [204] визначає національні правила та повноваження компетентного наглядового органу у сфері електронної ідентифікації та довірчих послуг, зокрема визначено, що національним наглядовим органом за довірчими послугами є Agency for Digitisation (Digitaliseringsstyrelsen). Відповідно закон формує правову основу безпечної електронної ідентифікації та довірчих послуг, які використовуються для доступу громадян і медичних працівників до цифрових державних та медичних сервісів;

- Закон про додаткові положення до Регламенту (ЄС) 2022/868 щодо європейського управління даними та про внесення змін до Регламенту (ЄС) 2018/1724 [202] визначає національні компетентні органи та встановлює додаткові правила щодо надання послуг посередництва даних, організацій з дата-альтруїзму та контролю за дотриманням вимог європейського законодавства про управління даними;

- Закон про додаткові положення до Регламенту щодо гармонізованих правил справедливого доступу до даних та їх використання [198] визначає, що Digitaliseringsstyrelsen визначено компетентним органом Данії та наділено повноваженнями щодо нагляду, отримання інформації, розгляду скарг та застосування заходів впливу;

- Консолідований закон Данії № 682 від 29 травня 2023 року про медичні вироби [103] встановлює національну правову основу для застосування законодавства ЄС щодо медичних виробів, зокрема Регламенту (ЄС) 2017/745 (MDR) та Регламенту (ЄС) 2017/746 (IVDR). Закон регулює, зокрема, вимоги до безпеки та якості, реєстрацію виробників і дистриб'юторів, клінічні випробування, повідомлення про інциденти, державний нагляд і контроль;

- Закон про забезпечення виконання Регламенту Європейського Парламенту і Ради про єдиний ринок цифрових послуг [201] доповнює Регламент (ЄС) 2022/2065 (Digital Services Act, DSA) та встановлює національний механізм його правозастосування в Данії, зокрема визначає Danish Agency for Digital Government (Digitaliseringsstyrelsen) компетентним органом і координатором цифрових послуг, встановлюючи повноваження щодо нагляду, приписів, штрафів та інших заходів примусового виконання. Для цифрової системи охорони здоров’я цей акт має опосередковане значення: він регулює цифрові платформи та посередницькі онлайн-сервіси, які можуть використовуватися для поширення медичної інформації, цифрових медичних сервісів та взаємодії пацієнтів із цифровим середовищем.

- Закон про додаткові положення до Регламенту Європейського Парламенту і Ради про цифрові ринки [197] наділяє Danish Competition and Consumer Authority (Konkurrence- og Forbrugerstyrelsen) статусом національного компетентного органу відповідно до статті 38 DMA та повноваженнями щодо проведення розслідувань і сприяння Європейській Комісії у забезпеченні виконання регламенту. Орган може самостійно або за скаргою досліджувати можливі порушення статей 5, 6 і 7 DMA на території Данії та передавати результати такого розслідування Європейській Комісії;

- Закон про додаткові положення до Регламенту про штучний інтелект [203] доповнював Регламент (ЄС) 2024/1689 (AI Act) та встановлював національні механізми його застосування в Данії, зокрема, визначав Digitaliseringsstyrelsen, Datatilsynet та Domstolsstyrelsen національними компетентними органами щодо нагляду, контролю та санкцій за порушення вимог AI Act. Станом на 16 серпня 2026 року Закон № 467 уже втратив чинність 2 серпня 2026 року. Його замінив новий датський закон про додаткові положення до AI Act, оскільки саме з 2 серпня 2026 року почала застосовуватися основна частина AI Act.

Цифрова трансформація системи охорони здоров'я Данії ґрунтується на комплексній та взаємопов'язаній нормативно-правовій базі, що поєднує спеціальне медичне законодавство з вимогами ЄС у сфері захисту даних, кібербезпеки, цифрової ідентифікації, управління даними та штучного інтелекту. Важливим напрямом сучасної реформи є формування Digital Sundhed Danmark та посилення централізованої координації цифрової інфраструктури й медичних даних. Водночас значна увага приділяється кібербезпеці та захисту персональних даних як ключовим передумовам безпечного функціонування цифрової системи охорони здоров'я. Таким чином, данська модель характеризується високим рівнем нормативної інтеграції з правом ЄС, централізацією управління цифровими ресурсами та орієнтацією на забезпечення безпеки, сумісності й доступності цифрових медичних послуг.

Система суб'єктів цифрової трансформації та кібербезпеки охорони здоров'я Данії має багаторівневу та координаційну структуру, що поєднує державні органи, регіони, муніципалітети та спеціалізовані цифрові й кібербезпекові установи. Її особливістю є поєднання централізованого управління цифровими даними та інфраструктурою через Данське управління даними охорони здоров'я і майбутню організацію Digital Sundhed Danmark із децентралізованою реалізацією цифрових послуг

регіонами та муніципалітетами. Кібербезпека забезпечується окремою спеціалізованою системою, що включає Центр кібербезпеки Данії, SundCERT, DCISSund, SAC та SOC. Така модель забезпечує розподіл повноважень, одночасно підтримуючи єдині стандарти цифрової взаємодії, централізовану координацію даних та оперативне реагування на кіберзагрози.

Естонія. Ключовими нормативно-правовими актами, які регулюють цифрову трансформацію системи охорони здоров'я Естонії, є наступні:

- Закон про організацію медичних послуг [173] – ключовий нормативно-правовий акт для цифрової трансформації системи охорони здоров'я, що визначає правові засади функціонування Системи інформації про здоров'я (Health Information System), включаючи склад медичних даних, порядок їх передачі, доступу, обробки та ведення журналів доступу;
- Закон про захист персональних даних [233] доповнює та конкретизує застосування GDPR в Естонії, встановлюючи національні правила обробки персональних даних, у тому числі спеціальних категорій даних, до яких належать медичні дані;
- Закон про публічну інформацію [251] визначає загальні правила створення, функціонування та доступу до державних інформаційних систем і баз даних, що для охорони здоров'я має значення через регулювання державної інформаційної інфраструктури, у складі якої функціонує Health Information System;
- Закон про електронні комунікації [142] регулює електронні комунікаційні мережі та послуги, що формують технологічну основу для функціонування цифрових державних і медичних сервісів та забезпечує надійність та безпеку цифрової інфраструктури;

- Закон про кібербезпеку [123] встановлює національні вимоги щодо забезпечення кібербезпеки, управління кіберризиками та повідомлення про інциденти, що має безпосереднє значення для захисту критичної цифрової інфраструктури, включаючи системи, пов'язані з охороною здоров'я;

В Естонії сформовано комплексну нормативно-правову основу цифрової трансформації системи охорони здоров'я, яка охоплює цифрові медичні дані, електронні комунікації, цифрову ідентифікацію, захист персональних даних та кібербезпеку. Національне законодавство доповнюється положеннями NIS2, GDPR, eIDAS, Data Governance Act, Data Act, AI Act, MDR та IVDR, що забезпечує узгодження цифрової охорони здоров'я Естонії з європейськими стандартами.

Інституційна модель цифрової трансформації системи охорони здоров'я Естонії характеризується чітким розподілом повноважень між органами формування політики, операторами цифрової інфраструктури, суб'єктами управління медичними даними та органами кібербезпеки і захисту інформації. Ключову роль у цифровій трансформації відіграють Міністерство соціальних справ, TEHIK, RIA та Tervisekassa, тоді як Health Information System формує технологічну основу обміну медичними даними. Водночас Andmekaitse Inspektsioon забезпечує контроль за захистом персональних даних, а CERT-EE - реагування на кіберінциденти, що формує багаторівневу систему управління цифровими ризиками. Така модель забезпечує інтеграцію цифрових медичних послуг, централізоване управління медичними даними та поєднання цифровізації з вимогами щодо їх захисту і кібербезпеки.

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. Перспективним також є розвиток єдиної цифрової інфраструктури медичних даних, забезпечення її сумісності, посилення секторної кібербезпеки та запровадження механізмів безпечного використання медичних даних і технологій штучного інтелекту.

Висновки до 4-го розділу

1. Встановлено, що Європейський Союз 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.

2. Аналіз еволюції нормативно-правового регулювання цифрової трансформації охорони здоров’я в Європейському Союзі 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.

3. Результатом цієї еволюції є цілісна система нормативно-правових актів, 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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. Перспективним також є розвиток єдиної цифрової інфраструктури медичних даних, забезпечення її сумісності, посилення секторної кібербезпеки та запровадження механізмів безпечного використання медичних даних і технологій штучного інтелекту.

РОЗДІЛ 5
УДОСКОНАЛЕННЯ МЕХАНІЗМІВ ДЕРЖАВНОГО УПРАВЛІННЯ ПРОЦЕСАМИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я

5.1. Механізм адаптації державного управління цифровою трансформацією системи охорони здоров'я до вимог Європейського Союзу

Цифрова трансформація національної системи охорони здоров'я не може відбуватися без врахування внутрішніх та зовнішніх соціально-економічних, політико-правових та культурно-ментальних факторів. «Державна політика цифрового розвитку визначає, як держава інтегрує новітні технології в усі сфери життя. У процесах цифровізації постає потреба у виробленні системної державної політики, яка має бути підтверджена досвідом розвинутих країн, що пройшли значний шлях у цьому напрямку та мають напрацювання з впровадження інструментів державного регулювання» [9].

Важливим фактором цифрової трансформації системи охорони здоров'я є євроінтеграційні процеси, саме тому будь-які державні реформи, які обумовлені соціально-економічними чи техніко-технологічними факторами, мають відбуватися у відповідності з євроінтеграційними процесами. У свою чергу цифрова трансформація системи охорони здоров'я стала пріоритетом державної політики як мінімум з двох причин: по-перше, цифрова трансформація суспільних відносин стала двигуном прогресу та розвитку економіки; по-друге, цифрова трансформація є вимогою Європейського Союзу, адже кожна національна система охорони здоров'я має інтегруватися в європейський єдиний інформаційний медичний простір. «Україна,

враховуючи реалії воєнного стану та особливості реформування системи охорони здоров'я, може адаптувати найкращі практики країн ЄС, включаючи партисипативне управління, цифрову етику та медичну кібербезпеку. Участь у транснаціональних проєктах і платформах може сприяти ефективному обміну досвідом» [79]. Зазначене актуалізує потребу розробки механізму адаптації державного управління цифровою трансформацією системи охорони здоров'я до вимог Європейського Союзу.

Зазначені питання частково досліджувалися вітчизняними вченими: 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.

«Широке впровадження цифрових рішень у медичній галузі стало важливим елементом модернізації європейських систем охорони здоров'я та забезпечило більш повне використання потенціалу новітніх технологій, що лежать в основі цих систем. Цифрова трансформація сприяє підвищенню ефективності державного управління медичною галуззю, що в свою чергу відіграє ключову роль у забезпеченні всебічного доступу до послуг охорони здоров'я. Цифрові технології можуть бути застосовані у навчанні, епіднагляді, забезпеченні безпеки здоров'я та наданні допомоги тим групам населення, які найбільше її потребують. Важливо зазначити, що ці підходи сприяють також розширенню прав та можливостей місцевих громад та громадян у покращенні власного здоров'я та рівня благополуччя» [9].

Формування механізму адаптації державного управління процесами цифрової трансформації системи охорони здоров'я до вимог Європейського Союзу має відбуватися в контексті правової оцінки Директив та Регламентів ЄС, а також аналізу досягнень України в цьому напрямку і прогалин реформування. Це дозволить визначити напрями формування та реалізації державно-управлінських рішень (таблиця 5.1).

Відповідно до представлених даних стан відповідності державного управління цифровою трансформацією системи охорони здоров'я вимогам ЄС характеризується наступними положеннями:

- щодо приведення національного законодавства до вимог Регламенту (ЄС) 2025/327 про Європейський простір даних охорони здоров'я (EHDS) варто наголосити, що Україна вже має значну частину базової цифрової інфраструктури, необхідної для подальшого наближення до моделі EHDS, насамперед функціонуючу ЕСОЗ, централізовану базу медичних даних та цифровий доступ пацієнтів. Водночас ключовими напрямами подальшої гармонізації є вторинне використання медичних даних, семантична та технічна сумісність, механізми управління доступом до даних і створення національної точки контакту з електронного здоров'я.

- рівень відповідності національного законодавства вимогам Регламенту (ЄС) 2024/1689 про штучний інтелект (AI Act) є ще недостатнім. Так, в Україні вже сформовано базові передумови для розвитку штучного інтелекту, зокрема затверджено Концепцію розвитку штучного інтелекту та започатковано механізми тестування ШІ-рішень. Водночас відсутність спеціального правового регулювання медичного ШІ, класифікації систем за рівнем ризику, вимог до валідації даних, людського контролю та національного органу нагляду свідчить про необхідність подальшої гармонізації законодавства України з вимогами AI Act.

Таблиця 5.1

Відповідність правових, інституційних та організаційних положень державного управління цифровою трансформацією системи охорони здоров'я

Нормативний акт ЄС	Досягнення	Прогалини
1	*2*	*3*
Регламент (ЄС) 2025/327 про Європейський простір даних охорони здоров'я (EHDS)	- внесення змін до Закону України «Основи законодавства України про охорону здоров'я» [35], що нормативно закріплюють функціонування Електронної системи охорони здоров'я (ЕСОЗ)	- замість європейської процедури самодекларування та відповідності технічним специфікаціям EHDS, в Україні діє локальний порядок підключення МІС через тестування ДП «Електронне здоров'я»
	- затверджено Порядок функціонування ЕСОЗ, реєстрів та правила доступу до них Постановою КМУ від 25.04.2018 № 411 [11]	- не врегульований на законодавчому рівні порядок анонімізації та надання даних для науковців і стартапів
	- схвалено Стратегію розбудови телемедицини, Розпорядженням КМУ від 14.07.2023 № 625-р [56], що затверджує перехід до єдиного цифрового телемедичного простору	- відсутня процедура реалізації права пацієнта відмовитися від передачі його деперсоналізованих даних для наукових чи статистичних досліджень
	- забезпечення функціонування понад 35 млн медичних карт, рецептів та висновків, що містяться в Центральній базі даних (ЦБД) ЕСОЗ [14]	- незавершений процес впровадження стандарту SNOMED CT для забезпечення сумісності та інтеграції
	- реалізація доступу громадян до своїх цифрових медичних даних (медичні сертифікати, кабінет пацієнта) через Портал та застосунок Дія [12]	- відсутній орган, відповідальний за видачу дозволів (*Data Permits*) на вторинне використання даних
	- запровадження інструментів відкритої звітності щодо медичних послуг та виплат через аналітику та дашборди НСЗУ [2]	- відсутня національна точка контакту з електронного здоров'я
Регламент (ЄС) 2024/1689 про штучний інтелект (AI Act)	- затвердження Концепції розвитку штучного інтелекту в Україні розпорядженням КМУ від 02.12.2020 № 1556-р [55]	- відсутня законодавча вимога (аналог ст. 14 AI Act), яка гарантує, що остаточне медичне рішення приймає лікар, а алгоритм виступає лише інструментом підтримки дій
	- розробка Дорожньої карти з регулювання штучного інтелекту Міністерством цифрової трансформації України [28]	- відсутні стандартизовані вимоги до валідації медичних датасетів та перевірки некоректних алгоритмічних упереджень
	- впровадження нейромереж для автоматизованого аналізу КТ-знімків та рентгенограм (для виявлення ознак інсульту, туберкульозу чи мінно-вибухових травм у закладах охорони здоров'я) [70]	- відсутні нормативні вимоги щодо кваліфікації медичних ШІ-систем за рівнями ризику (неприйнятний, високий, обмежений, мінімальний), як це вимагається статтями Регламенту

Продовження табл. 5.1

1	*2*	*3*
	- впровадження Мінцифрою спеціальних правових режимів для тестування стартапів та продуктів на базі ШІ [13]	- відсутній національний компетентний орган з нагляду за ШІ
Регламент (ЄС) 2016/679 про захист даних (GDPR)	- наявність законодавчого регулювання захисту персональних даних (Закон України «Про захист персональних даних»; Закон України «Про захист інформації в інформаційно-комунікаційних системах») [48]	- у законодавстві відсутні або некоректно сформульовані такі ключові поняття GDPR, як псевдонімізація, анонімізація, профілювання, контролер даних та процесор даних
		- функції нагляду виконує Департамент захисту персональних даних Офісу Омбудсмана, який не має достатніх ресурсів для ІТ-аудиту
	- центральна база даних ЕСОЗ має діючий атестат відповідності КСЗІ, виданий Держспецзв'язком, що гарантує високий рівень технічної безпеки та шифрування медичних даних [47]	- відсутність концепції «Приватності за замовчуванням», адже МІС проходять перевірку лише на функціональну відповідність ЕСОЗ
		- відсутність посади Офіцера із захисту даних в ЗОЗ
	- реалізовано функціонал «кабінету пацієнта» та розмежовано права доступу лікарів (доступ до історії хвороби можливий лише за наявності активного «терапевтичного зв'язку» та за згодою пацієнта через СМС-підтвердження)	- не закріплено процедуру DPIA щодо обробки медичних даних високого ризику
		- в архітектурі ЕСОЗ вилучення медичних записів є ускладненим через суворі вимоги щодо обов’язкового терміну зберігання медичної документації
		- низькі санкції за порушення захисту даних
Регламент (ЄС) №910/2014 про електронну ідентифікацію та довірчі послуги (eIDAS)	- Закон України «Про електронні довірчі послуги» [42] є базово гармонізований із Регламентом eIDAS та увів поняття КЕП, УЕП, електронної печатки, кваліфікованої позначки часу	- попри технічну готовність, двостороння угода про взаємне визнання довірчих послуг між Україною та ЄС перебуває на стадії фіналізації оцінки, тому український КЕП лікаря наразі автоматично не приймається у СОЗ країн ЄС без спеціальних двосторонніх мостів
	- було удосконалено законодавство для гармонізації з eIDAS у частині взаємного визнання електронних довірчих послуг між Україною та ЄС [38]	- у 2024 році ЄС прийняв оновлення eIDAS 2.0, яке вводить Європейський гаманець цифрової ідентичності (EUDI Wallet), відповідно «Дія» потребує гармонізації архітектури Wallet із технічними специфікаціями ARF (Architecture and Reference Framework) ЄС, зокрема для збереження електронних медичних рецептів та атрибутів лікаря
	- 100 % медичних працівників, які працюють з Електронною системою охорони здоров'я (ЕСОЗ), застосовують КЕП для підписання медзаписів, рецептів та направлень	

Продовження табл. 5.1

1	*2*	*3*
	- у застосунку «Дія» та Дія.Підпис реалізувало цифрові паспорти та сумісний з eIDAS підпис (EU-compliant), що фактично відповідає високому рівню впевненості	- КЕП підтверджує особу та сертифікат ключа, але не завжди інтегрований із реальними реєстрами ліцензій МОЗ/Реєстром медичних працівників на момент підписання документа за кордоном
	- Україна створила та підтримує Національний довірений список електронних довірчих послуг, який формується за стандартами ЄС [73]	- деякі лікарні все ще використовують застарілі файлові ключі замість захищених носіїв
Регламент (ЄС) 2022/868 про європейське управління даними (DGAct)	- Закон України «Про доступ до публічної інформації» [41]: Регламентує відкриті дані та обов'язок розпорядників надавати доступ до публічних масивів	- відсутній чіткий механізм, який дозволив би науковцям чи MedTech-стартапам законно запитувати доступ до деперсоналізованих первинних даних ЕСОЗ у закритому, захищеному середовищі
	- Закон України «Про публічні електронні реєстри» [52] встановив єдині рамки для створення та функціонування публічних реєстрів, включаючи реєстри ЕСОЗ	- відсутній правовий статус Посередників з надання послуг обміну даними (Data Sharing Services), а також правила їх сертифікації та нагляду
	- МОЗ та НСЗУ активно публікують деперсоналізовані масиви медичних даних (агрегована статистика захворюваності, дані про аптеки, виконання програми «Доступні ліки»).	- немає правового статусу «Визнаних в ЄС організацій альтруїзму щодо даних» та відсутній єдиний реєстр таких організацій
	- функціонує Дія.Engine, що є державною платформою для розгортання реєстрів, яка дозволяє уніфі-кувати структуру обміну даними між відомствами	- відсутність компетентних органів з питань управління даними (Competent Bodies for Data Governance)
Регламент (ЄС) 2023/2854 про правила доступу до даних (Data Act)	- Закон України «Про публічні електронні реєстри» [52] закріпив базові принципи інтероперабельності та автоматизованого обміну даними між реєстрами через систему «Трембіта».	- неврегульовано право пацієнта / користувача на доступ до даних пристрою та право на передачу даних третім особам
	- спеціальний правовий режим Дія.City [54] створив сприятливі умови для розвитку українських MedTech-компаній та розробників IoT-пристроїв	- невизначеність щодо доступу органів влади у випадках надзвичайного стану
	- масове підключення сучасного діагностичного обладнання у закладах охорони здоров'я до Медичних інформаційних систем (МІС) за міжнародним стандартом DICOM	- бар’єри при зміні постачальників хмарних медичних послуг

Продовження табл. 5.1

1	*2*	*3*
Директива (ЄС) 2022/2555 про заходи щодо забезпечення високого загального рівня кібербезпеки (NIS2)	- Закон України «Про основні засади забезпечення кібербезпеки України» [51] визначив правові основи захисту критичної інфраструктури та створив Національний координаційний центр кібербезпеки (НКЦК)	- в Україні до критичної інфраструктури відносять переважно великі високоспеціалізовані лікарні або центральні компоненти ЕСОЗ, у свою чергу NIS2 класифікує як Essential/Important Entities практично всі заклади охорони здоров'я (включаючи приватні клініки), виробників фармацевтичної продукції, критичних медичних виробів та біомедичні лабораторії
	- Закон України «Про критичну інфраструктуру» [49] включив сектор охорони здоров'я до переліку життєво важливих секторів критичної інфраструктури держави	- строки інформування про кібератаки в галузі охорони здоров'я юридично не деталізовані з такою точністю, передбаченою NIS2
	- при МОЗ та ДП «Електронне здоров'я» функціонують підрозділи кібербезпеки, що здійснюють моніторинг загроз ЕСОЗ та взаємодіють із CERT-UA	- перевірка постачальників МІС здебільшого обмежується формальною наявністю атестата КСЗІ, без постійного контролю ланцюга розробки
	- медичні інформаційні системи, які підключаються до ЕСОЗ, зобов'язані побудувати Комплексну систему захисту інформації (КСЗІ) та отримати атестат відповідності від Держспецзв'язку	- відповідальність керівників закладів охорони здоров'я за кібербезпеку має переважно декларативний характер
Регламент (ЄС) 2019/881 про Агентство ЄС з кібербезпеки та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій (Cybersecurity Act)	- Закон України «Про технічні регламенти та оцінку відповідності» [57] встановлює єдині правові та організаційні засади розроблення, прийняття та застосування технічних регламентів і процедур оцінки відповідності	- сертифікація КСЗІ є суто національним формалізованим інструментом, який не визнається в ЄС, де запроваджено загальноєвропейські схеми сертифікації з трьома рівнями довіри: базовий (basic), середній (substantial) та високий (high).
	- Національний орган із сертифікації та захисту (Держспецзв'язку) здійснює регулювання та видачу атестатів відповідності Комплексної системи захисту інформації (КСЗІ) для ЕСОЗ та МІС	- кожна держава повинна призначити Національний орган із сертифікації кібербезпеки, в той час як в Україні ці функції розпорошені між НААУ та Держспецзв'язку без прямої прив'язки до європейських схем сертифікації
	- медична інформаційна система не може бути підключена до Центральної бази даних ЕСОЗ без успішного проходження державної експертизи КСЗІ та отримання атестата відповідності	- кібербезпека підключеного медичного обладнання перевіряється переважно на рівні загальної електромагнітної сумісності та безпеки медичних виробів, але не проходить повноцінної перевірки стійкості до кібератак за стандартами CSA

Продовження табл. 5.1

1	*2*	*3*
	- укладено робочу угоду з Агентством ЄС з питань кібербезпеки (ENISA) про обмін оперативними даними щодо кіберзагрози та інцидентів	- процедура отримання КСЗІ є однаково бюрократизованою та тривалою як для великих хмарних систем, так і для простих модулів МІС
Регламент (ЄС) 2024/2847 про горизонтальні вимоги до кібербезпеки продуктів з цифровими елементами (Cyber Resilience Act)	- Технічний регламент щодо медичних виробів [45] встановлює загальні вимоги до безпеки, якості та оцінки відповідності медичного обладнання перед випуском у цивільний обіг	- Технічний регламент щодо медичних виробів [45] оцінює переважно фізичну, функціональну та електромагнітну безпеку медвиробів, але не містить обов’язкових вимог щодо аудиту вихідного коду, архітектурного загартування ПЗ та захисту від вразливостей на етапі розробки
		- відсутня вимога до розробників MedTech та МІС надавати специфікацію програмних компонентів
	- функціонування CERT-UA та галузевих підрозділів кіберзахисту, що здійснюють моніторинг загроз для критичної інфраструктури	- невизначено часового регламенту (наприклад, 24 години за CRA), протягом якого виробник медичного пристрою чи ПЗ зобов'язаний випустити та доставити патч безпеки для виявленої критичної вразливості
		- виробники не зобов'язані за законом гарантувати підтримку оновленнями безпеки протягом усього очікуваного строку служби пристрою
Регламент (ЄС) 2017/745 про медичні вироби (MDR) Регламент (ЄС) 2017/746 про медичні вироби для діагностики in vitro (IVDR)	- Технічний регламент щодо медичних виробів [45] та Технічний регламент щодо медичних виробів для діагностики in vitro [46] імплементували попередні Директиви ЄС (93/42/ЕЕС та 98/79/ЕС) і створили основу для процедур оцінки відповідності	- застаріла класифікація Програмного забезпечення як медичного виробу
		- відсутність вимог щодо постійної клінічної оцінки та постмаркетингового нагляду
	- Закон України «Про державний ринковий нагляд і контроль нехарчової продукції» [40] та Закон України «Про загальну безпечність нехарчової продукції» [44] визначили повноваження Держлікслужби щодо здійснення ринкового нагляду, перевірки відповідності маркування та простежуваності ланцюгів постачання медвиробів.	- відсутність національної бази UDI та інтеграції з EUDAMED

Продовження табл. 5.1

1	*2*	*3*
	- забезпечено технічну можливість інтеграції Лабораторних інформаційних систем (ЛІС) із Центральною базою даних ЕСОЗ для передачі результатів IVD-тестувань із використанням міжнародного кодифікатора LOINC у рамках виконання Закону України «Про публічні електронні реєстри» [52]	- невідповідність вимог до оцінки систем діагностики in vitro
Регламент (ЄС) 2022/2065 про єдиний ринок цифрових послуг (Digital Services Act); *- Регламент (ЄС) 2022/1925 про конкурентні та чесні ринки в цифровому секторі (Digital Markets Act)*	- Закон України «Про електронну комерцію» [43] встановив базові правові засади функціонування онлайн-торгівлі та інформаційних послуг	- відсутність градації відповідальності онлайн-платформ (DSA), зокрема відсутній чіткий розподіл суб'єктів на прості хостинг-провайдери, онлайн-платформи та дуже великі онлайн-платформи (VLOPs), адже за вимогами DSA, великі сервіси запису до лікарів чи онлайн-аптеки зобов'язані проводити аудит системних ризиків (зокрема ризиків поширення фальсифікованих ліків або недоведеної медичної інформації)
	- Закон України «Про медіа» [50] запровадив перші елементи регулювання онлайн-платформ, спільного регулювання та протидії дезінформації у цифровому просторі	
	- Закон України «Про внесення змін до статті 19 Закону України "Про лікарські засоби" щодо дистанційної торгівлі лікарськими засобами» [39] легалізував та врегулював діяльність електронних аптек та ліцензованих маркетплейсів ліків	- відсутність процедури «Notice and Action» та захисту від фальсифікату
		- проблеми прив'язки користувачів та відсутності сумісності
		Відсутність регулювання «гейткіперів» у сфері eHealth/MedTech
		непрозорість алгоритмів рекомендацій та таргетованої реклами

- сьогодні в Україні сформовано правові та технічні положення для захисту персональних і медичних даних, функціонування ЕСОЗ, розмежування доступу та застосування технічних засобів захисту інформації (Закон України «Про захист персональних даних», Закон України «Про захист інформації в інформаційно-комунікаційних системах»). Водночас чинне регулювання ще не повною мірою відповідає підходам GDPR, зокрема в частині понятійного апарату, принципів «приватності за замовчуванням», проведення оцінки впливу на захист даних (DPIA) та інституційної спроможності органу нагляду. Додаткового вдосконалення потребують питання призначення відповідальних за захист даних у закладах охорони здоров'я, регламентації обробки високоризикових медичних даних та підвищення рівня відповідальності за порушення вимог щодо їх захисту. Відповідне наближення законодавства до GDPR є необхідною умовою подальшої інтеграції української цифрової системи охорони здоров'я до європейського цифрового простору.

- для відповідності нормам Регламент (ЄС) №910/2014 про електронну ідентифікацію та довірчі послуги (eIDAS) сформовано базову правову та технічну основу для електронної ідентифікації та довірчих послуг (Закон України «Про електронні довірчі послуги»), а КЕП широко використовується медичними працівниками під час роботи з ЕСОЗ; також функціонує Національний довірчий список електронних довірчих послуг. Водночас повна відповідність eIDAS 2.0 потребує завершення взаємного визнання українських довірчих послуг з ЄС, подальшої інтеграції «Дії» з архітектурою EUDI Wallet, а також модернізації засобів зберігання ключів і забезпечення надійного зв'язку електронної ідентифікації з професійними реєстрами медичних працівників.

- щодо відповідності нормам Регламенту (ЄС) 2022/868 про європейське управління даними (DGAct) варто наголосити, що в Україні сформовано правову базу та техніко-технологічне забезпечення для

відкритого доступу й управління даними, зокрема через Закон України «Про доступ до публічної інформації», Закон України «Про публічні електронні реєстри» та платформу Дія.Engine. В той же час невирішеними залишаються питання: 1) врегулювання безпечного доступу до деперсоналізованих медичних даних для досліджень та інновацій; 2) правовий статус посередників і організацій альтруїзму щодо даних; 3) визначення компетентних органів у сфері управління даними.

- в контексті Data Act Україна вже має окремі елементи, необхідні для реалізації підходів, зокрема нормативно закріплену інтероперабельність реєстрів, систему «Трембіта», сприятливе середовище для розвитку цифрових і MedTech-рішень та практику використання DICOM у медичній інфраструктурі. Разом із тим законодавче поле потребує доопрацювання щодо прав користувача на дані, згенеровані підключеними медичними пристроями, умов їх передачі та використання державою, а також забезпечення реальної можливості зміни постачальників хмарних послуг.

- в Україні є нормативна та організаційна основа кіберзахисту медичної сфери, зокрема через законодавство про кібербезпеку й критичну інфраструктуру, вимоги КСЗІ для МІС та функціонування галузевих підрозділів кібербезпеки. Водночас для наближення до NIS2 необхідно розширити коло охоплених суб’єктів, деталізувати строки та процедури повідомлення про інциденти, посилити постійний контроль безпеки постачальників і ланцюгів розробки МІС та встановити реальну відповідальність керівників закладів охорони здоров’я за управління кіберризиками.

- в Україні сформовано базову систему технічного регулювання та сертифікації кібербезпеки, що забезпечує перевірку захищеності ЕСОЗ і МІС через механізми КСЗІ та діяльність Держспецзв’язку. Водночас

модель потребує наближення до Cybersecurity Act, зокрема шляхом запровадження сумісних з ЄС схем сертифікації, чіткого визначення національного органу з кіберсертифікації, поширення вимог на підключені медичні пристрої та переходу від переважно формального підтвердження відповідності до постійного ризик-орієнтованого контролю кібербезпеки.

- Регламент (ЄС) 2024/2847 про горизонтальні вимоги до кібербезпеки продуктів з цифровими елементами (Cyber Resilience Act) встановлює обов'язкові вимоги кібербезпеки для усіх продуктів з цифровими елементами (hardware та software), що виводяться на ринок ЄС. У сфері медицини CRA охоплює розумні медичні прилади, IoT-монітори, ПЗ для діагностики та Медичні інформаційні системи (МІС). Регламент зобов'язує виробників гарантувати безпеку продукту протягом усього його життєвого циклу (Security by Design/Default) та забезпечувати підтримку оновленнями безпеки щонайменше протягом 5 років. В Україні щодо його реалізації зроблені певні кроки щодо запровадження базових механізмів забезпечення безпеки цифрових медичних продуктів через Технічний регламент щодо медичних виробів та діяльність CERT-UA і галузевих підрозділів кіберзахисту. Щодо прогалин та перспективних напрямів реформування сьогодні є потреба у: 1) врегулюванні вимог до кібербезпеки програмного забезпечення на всьому життєвому циклі; 2) декларуванні програмних компонентів, своєчасному усуненню критичних вразливостей; 3) обов’язкової підтримки безпекових оновлень протягом строку експлуатації цифрових медичних продуктів.

- Україна має сформовану базову систему регулювання медичних виробів та IVD, зокрема через Технічні регламенти щодо медичних виробів і медичних виробів для діагностики in vitro, а також законодавство про ринковий нагляд; водночас уже створюються передумови для цифрової інтеграції лабораторних даних із ЕСОЗ із використанням LOINC. Водночас

для наближення до MDR та IVDR необхідно оновити класифікацію програмного забезпечення як медичного виробу, запровадити системний постмаркетинговий нагляд і клінічну оцінку, створити національну систему UDI та забезпечити інтеграцію з EUDAMED, а також удосконалити вимоги до оцінки IVD.

- якщо DSA фокусується на безпеці цифрового середовища, боротьбі з дезінформацією, деструктивним контентом та захисті прав користувачів цифрових послуг, то DMA регулює антимонопольні правила для великих цифрових платформ-гейткіперів (Gatekeepers), запобігаючи нав'язуванню монопольних сервісів та забезпечуючи відкриту конкуренцію. У сфері охорони здоров'я це безпосередньо стосується телемедичних платформ, великих агрегаторів запису до лікарів та брокерів медичних даних, а також онлайн-аптек та маркетплейсів ліків. В Україні сформовано окремі елементи правового регулювання цифрового середовища, зокрема електронної комерції, онлайн-платформ і дистанційної торгівлі лікарськими засобами, що створює основу для подальшого розвитку цифрових медичних сервісів. Водночас для наближення до DSA та DMA необхідно чіткіше розмежувати відповідальність різних типів онлайн-платформ, запровадити процедури Notice and Action, механізми контролю системних ризиків і прозорості алгоритмів, а також визначити правила щодо великих цифрових платформ та «гейткіперів» у сфері eHealth/MedTech.

Забезпечення усунення виявлених прогалин передбачає потребу в розробці сукупності організаційних, правових, інформаційних, фінансових та кадрових положень, які мають бути взаємопов’язаними. Для забезпечення зазначеного є потреба в побудові комплексного механізму державного управління цифровою трансформацією системи охорони здоров’я (табл. 5.2).

Таблиця 5.2

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 Portability)</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 анонімізація 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>Розділ 8. 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. 5.2

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 постій-ного 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 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
РОЗШИРЕННЯ ІНСТИТУЦІЙНОЇ СПРОМОЖНОСТІ ДЛЯ ЗАБЕЗПЕЧЕННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В МЕДИЦИНІ			
- утворення спеціалізованого суб'єкту державного управління, що виступатиме 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 забезпечення постмаркетингового 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 законопроєкт [60], 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, з прямим посиланням на спеціальне законодавство 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 HDAB.		- 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. 5.2

ПРИЙНЯТТЯ ЗАКОНУ УКРАЇНИ ПРО НАЦІОНАЛЬНУ КОМІСІЮ З ПИТАНЬ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ТА ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ			
- на сьогодні розглядається Верховною Радою новий законопроєкт [59], 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 права 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 Національної комісії (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	
РЕГЛАМЕНТ (ЄС) 2022/868 ПРО ЄВРОПЕЙСЬКЕ УПРАВЛІННЯ ДАНИМИ (DGACT)			
РОЗРОБКА ТА ПРИЙНЯТТЯ ЗАКОНУ УКРАЇНИ ПРО УПРАВЛІННЯ ДАНИМИ			
Розділ 1. Загальні положення	*Стаття 1.* Предмет та мета	*Стаття 2.* Сфера застосування	*Стаття 3.* Визначення термінів

Продовження табл. 5.2

Розділ 2. Повторне використання захищених даних публічного сектору	*Стаття 4.* Категорії даних, що підлягають повторному використанню		*Стаття 5.* Умови повторного використання
	Стаття 6. Безпечні середовища обробки		*Стаття 7.* Роль спеціалізованих органів
Розділ 3. Послуги з обміну даними (Посередники у сфері даних)	*Стаття 8.* Правовий статус посередників з обміну даними	*Стаття 9.* Принцип нейтральності посередників	*Стаття 10.* Реєстрація та нагляд
Розділ 4. Альтруїзм щодо даних	*Стаття 11.* Поняття та засади альтруїзму щодо даних	*Стаття 12.* Реєстр організацій альтруїзму щодо даних	*Стаття 13.* Згода на альтруїзм щодо даних
Розділ 5. Інституційний механізм та компетентні органи	*Стаття 14.* Національний компетентний орган з управління даними		*Стаття 15.* Рада з управління даними
Розділ 6. Міжнародне співробітництво та транскордонна передача	*Стаття 16.* Транскордонний обмін даними		*Стаття 17.* Заходи протизаконного доступу третіх країн
Розділ 7. Відповідальність та нагляд	*Стаття 18.* Розгляд скарг та позасудове вирішення спорів		*Стаття 19.* Санкції за порушення Закону
Розділ 8. Прикінцеві та перехідні положення	Внесення змін до Законів України		Перехідний період
РОЗШИРИТИ ІНФРАСТРУКТУРНУ СПРОМОЖНІСТЬ УПРАВЛІННЯ ДАНИМИ			
- 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		- розробка та реалізація Державного реєстру організацій альтруїзму щодо даних	
РЕГЛАМЕНТ (ЄС) 2023/2854 ПРО ПРАВИЛА ДОСТУПУ ДО ДАНИХ (DATA ACT)			
ПРАВОВЕ ВРЕГУЛЮВАННЯ ТЕХНІЧНОГО ХАРАКТЕРУ ЩОДО ДОСТУПУ ДО ДАНИХ			
гармонізація Технічного регламенту щодо медичних виробів	***розробка та прийняття закону України про управління даними***		***уніфікація стандартів міграції для Медичних інформаційних систем***
- внесення змін до Постанови КМУ № 753 Про затвердження Технічного регламенту щодо медичних виробів [45] 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 DICOM	- передбачити 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		- затвердження МОЗ обов'язкових вимог до сумісності та безперешкодного вивантаження баз даних лікарень у разі зміни оператора МІС чи хмарного дата-центру

Продовження табл. 5.2

<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 чіткого регламенту сповіщення CSIRT/CERT-eHealth та Держспецзв'язку про кіберінциденти за 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 заходів 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. 5.2

<table>
<tr><th colspan="6">РЕГЛАМЕНТ (ЄС) 2017/745 ПРО МЕДИЧНІ ВИРОБИ (MDR) ТА РЕГЛАМЕНТ (ЄС) 2017/746 ПРО МЕДИЧНІ ВИРОБИ ДЛЯ ДІАГНОСТИКИ IN VITRO (IVDR)</th></tr>
<tr><td colspan="6">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</td></tr>
<tr><td colspan="2">- включити чітке визначення SaMD (Software as a Medical Device) як самостійного медичного виробу</td><td colspan="2">- гармонізувати періоди переходів для існуючих виробів відповідно до строків ЄС (до 2027/2028 років залежно від класу ризику)</td><td colspan="2">- внести до Додатка класифікаційних критеріїв нового Технічного регламенту Правило, яке перерозподіляє класи ризику для ПЗ</td></tr>
<tr><td colspan="6">ВНЕСТИ ЗМІНИ ДО ПОСТАНОВИ КМУ ЩОДО ВЕДЕННЯ ДЕРЖАВНОГО РЕЄСТРУ МЕДИЧНОЇ ТЕХНІКИ ТА ВИРОБІВ</td></tr>
<tr><td colspan="3">- 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)</td><td colspan="3">- зобов'язати Держлікслужбу забезпечити технічну сумісність (API) національного реєстру з європейською базою EUDAMED</td></tr>
<tr><td colspan="6">ЗАТВЕРДИТИ «ПОРЯДОК ПРОВЕДЕННЯ ПІСЛЯРИНКОВОГО КЛІНІЧНОГО СПОСТЕРЕЖЕННЯ (PMCF) ТА СПОСТЕРЕЖЕННЯ ЗА ФУНКЦІОНУВАННЯМ IVD (PMPF)»</td></tr>
<tr><td colspan="3">- зобов'язати розробників SaMD та ШІ-систем щорічно надавати до Держлікслужби Звіт із безпеки</td><td colspan="3">- для ШІ-систем у медицині зобов'язати виробників проводити регулярну перевірку точності роботи алгоритму на реальних українських клінічних даних</td></tr>
<tr><th colspan="6">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)</th></tr>
<tr><td colspan="6">РОЗРОБКА ТА ПРИЙНЯТТЯ ЗАКОНУ УКРАЇНИ «ПРО ЦИФРОВІ ПОСЛУГИ»</td></tr>
<tr><td>Розділ 1. Загальні положення</td><td colspan="2">Стаття 1. Предмет та мета</td><td colspan="2">Стаття 2. Сфера застосування</td><td>Стаття 3. Визначення термінів</td></tr>
<tr><td rowspan="2">Розділ 2. Відповідальність надавачів посередницьких цифрових послуг</td><td colspan="3">Стаття 4. Звільнення від відповідальності за передачу інформації</td><td colspan="2">Стаття 5. Кешування</td></tr>
<tr><td colspan="3">Стаття 6. Хостинг та зберігання даних</td><td colspan="2">Стаття 7. Заборона загального моніторингу</td></tr>
<tr><td rowspan="2">Розділ 3. Обов’язки щодо прозорості та протидії протиправному контенту</td><td colspan="3">Стаття 8. Механізми сповіщень про наявність протиправного контенту</td><td colspan="2">Стаття 9. Обґрунтування рішень у разі видалення контенту, блокування акаунту чи обмеження доступу</td></tr>
<tr><td colspan="3">Стаття 10. Інститут довірених сповіщувачів</td><td colspan="2">Стаття 11. Позасудове вирішення спорів та внутрішні системи розгляду скарг</td></tr>
<tr><td rowspan="2">Розділ 4. Додаткові вимоги до онлайн-платформ та маркетплейсів</td><td colspan="3">Стаття 12. Належна перевірка продавців</td><td colspan="2">Стаття 13. Заборона маніпулятивних інтерфейсів</td></tr>
<tr><td colspan="3">Стаття 14. Прозорість рекомендаційних систем та реклами</td><td colspan="2">Стаття 15. Захист чутливих даних у таргетованій рекламі</td></tr>
</table>

Продовження табл. 5.2

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		

Запропонований комплексний механізм адаптації державного управління цифровою трансформацією системи охорони здоров'я до вимог Європейського Союзу визначає перехід від фрагментарної адаптації окремих актів до комплексної законодавчої архітектури цифрової охорони здоров'я, де окремими законами регулюються медичні дані, управління даними, ШІ та цифрові послуги, а спеціальні зміни вбудовують ці правила у чинне медичне, інформаційне та конкурентне законодавство. Запропонований механізм не зводиться до внесення окремих поправок у чинне законодавство, а передбачає структурну перебудову законодавства шляхом поєднання нових спеціальних законів, модернізації чинних законів і повного оновлення технічних регламентів, що створює правову основу для переходу від нинішньої моделі ЕСОЗ до європейсько-сумісної системи управління цифровою охороною здоров'я. Зокрема, пропонується розширення нормативно-правової бази шляхом прийняття нових законодавчих актів:

- Закон України «Про обіг медичних даних», що пропонується як базовий спеціальний закон, метою якого є створення самостійного правового режиму обігу медичних даних, який охоплює їх первинне і вторинне використання, права пацієнтів, транскордонний обмін, анонімізацію та псевдонімізацію, безпечні середовища обробки, доступ до даних, інтероперабельність, аудит, кібербезпеку та відповідальність, а також інституційно закріплює статус Національного органу з доступу до медичних даних (HDAB) та Національної точки контакту з електронного здоров'я (NCPH);

- Рамковий Закон України «Про штучний інтелект», що передбачає загальні правила використання технологій штучного інтелекту, а для охорони здоров'я доповнюється спеціальними вимогами до медичних ШІ-систем. Запропонована конструкція включає постійний моніторинг алгоритмів, стандарти підготовки медичних датасетів, регулювання високоризикових систем, інформування пацієнтів та порядок підключення і верифікації ШІ-модулів у ЕСОЗ;

- Закон України «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» має стати новим інституційним законом. Передбачені повноваження Комісії включають аудит алгоритмічної прозорості, контроль privacy by default, затвердження методологій DPIA для охорони здоров'я, реагування на витоки медичних даних, нагляд за дотриманням правил захисту даних під час вторинного використання та представництво України у відповідних європейських механізмах. Закон має сформувати незалежний наглядовий інститут, здатний працювати не лише з персональними даними загалом, а й зі специфічними ризиками цифрової медицини;

- Закон України «Про управління даними» - закон у сфері data governance, який має врегулювати повторне використання захищених даних публічного сектору, посередників з обміну даними, data altruism, компетентні органи, транскордонний обмін і відповідальність. У частині медицини він створює загальну правову рамку для безпечного повторного використання даних, на яку має спиратися спеціальний режим медичних даних. Окремо передбачено створення функціоналу для добровільного надання громадянами анонімізованих медичних даних для наукових та MedTech-проєктів і відповідного державного реєстру організацій data altruism;

- Закон України «Про цифрові послуги» має стати загальним правовим режимом посередницьких цифрових послуг та онлайн-платформ. Він охоплює відповідальність хостинг-провайдерів, Notice and Action, внутрішні механізми розгляду скарг, перевірку продавців, прозорість рекомендаційних систем, таргетованої реклами, системні ризики великих платформ, аудит і нагляд. Для eHealth/MedTech цей закон створює правове поле для регулювання онлайн-платформ, маркетплейсів, електронних аптек, пацієнтських сервісів та великих цифрових платформ.

Важливо зазначити, що 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 MIC та MedTech-рішень.

- Закон України «Про захист економічної конкуренції» передбачає зміни, спрямовані наспрямовані на цифрових гейткіперів. 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 заміни 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.

Запропонована інституційна архітектура перетворює систему охорони здоров'я з простого користувача цифрових рішень на суворо регульований, безпечний та високотехнологічний ринок даних і ШІ-технологій, здатний до

повної інтеграції в єдиний цифровий простір Європейського Союзу. Більш детально функціонування запропонованих суб'єктів державного управління буде розглянуто в наступних дослідженнях.

Таким чином, здійснено комплексний аналіз стану відповідності вітчизняної системи державного управління цифровою трансформацією охорони здоров'я регуляторним актам Європейського Союзу та розроблено механізм її адаптації. Сформований підхід спрямований на подолання суттєвого розриву між наявною інфраструктурою електронної системи охорони здоров'я і європейськими директивами та регламентами. Для вирішення зазначеної проблеми запропоновано структуру та змістовне наповнення сукупності нових нормативно-правових актів, зокрема: Закон 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.

5.2. Державне регулювання використання технологій штучного інтелекту у функціонуванні системи охорони здоров'я

Технології штучного інтелекту увійшли у всі сфери суспільного життя, в тому числі в охорону здоров'я. Сьогодні є можливість, на усіх етапах організації системи охорони здоров'я та надання медичної допомоги, застосувати технології штучного інтелекту. Їх використання дозволяє підвищити ефективність функціонування системи охорони здоров'я та запроваджувати інноваційні методи надання медичних послуг. Впровадження технологій штучного інтелекту визначає майбутнє системи охорони здоров'я як на рівні управлінських процесів, так і на рівні медичних. «Штучний інтелект є не просто інструментом - він стає повноцінним партнером медичного фахівця. Його роль у майбутньому охороні здоров'я складно переоцінити» [7]. Відповідно процеси використання технологій штучного інтелекту в медицині стають об'єктом державного управління, нормативно-правового регулювання, соціально-економічних процесів. Це актуалізує науковий пошук вирішення сукупності проблем державного регулювання використання технологій штучного інтелекту у функціонуванні системи охорони здоров'я.

Зазначені проблеми частково досліджували вітчизняні вчені, зокрема: Д.О. Грицишен, Л.В. Сергієнко, Л.В. Антонова, С.М. Петрик, А.А. Висоцький, О.О. Суріков, С.В. Василюк-Зайцева, В.В. Мельник, В.В. Кривецький, Д.В. Проняєв, М.С. Саєнко, А.В. Вовк, М.І. Мойсеєнко, М.М. Кузишин, Л.В. Туровська, Ю.С. Мазуренко, М.Л. Петришин, О.І. Пархоменко-Куцевіл та інші. Серед зарубіжних вчених питання штучного інтелекту в медицині розвивали: Тімо Мінссен (Timo Minssen), Еффі Ваєна (Effy Vayena), І Гленн Коен (I Glenn Cohen), Єлена Шмід (Jelena Schmidt)т), Нінке М. Шутте (Nienke M Schutte), Стефан Буттідже (Stefan

Buttigieg), Девід Новілло-Ортіс (David Novillo-Ortiz), Ерік Сазерленд (Eric Sutherland), Майкл Андерсон (Michael Anderson), Барт де Вітте (Bart de Witte), Майкл Пеолссон (Michael Peolsson), Бригід Унім (Brigid Unim), Мілена Павлова (Milena Pavlova), Аріель Дора Стерн (Ariel Dora Stern), Еліас Моссіалос (Elias Mossialos), Робін ван Кессел (Robin van Kessel), Віда Фернандес, Хосе (Vida Fernandez Jose), Тімо Мінссен (Timo Minssen), Сара Герке (Sara Gerke), Матео Абой (Mateo Aboy), Ніколсон Прайс (Nicholson Price), Гленн Коен (Glenn Cohen), Дженніфер Віберг Йоханссон (Jennifer Viberg Johansson), Санта-Слокенберга (Santa Slokenberga) та інші.

«Штучний інтелект відіграє ключову роль у трансформації медицини, сприяючи підвищенню точності діагностики, оптимізації лікувальних процесів і зниженню витрат. Ринок ШІ в медицині демонструє стабільне зростання, що зумовлено технологічним прогресом і щораз вищим попитом на автоматизовані рішення. Подальший розвиток штучного інтелекту відкриває нові можливості для персоналізованої медицини та ефективного управління медичними даними» [10].

«Термін ШІ вперше введений групою вчених на конференції, що відбулася 1956 р. в Дартмутському коледжі (Нью-Гемпшир, США). Їх метою було розробити комп’ютерні системи, здатні виконувати завдання, які зазвичай потребують людського інтелекту. Міністерство оборони США інвестувало значні кошти в декілька проєктів, які зрештою були припинені через недооцінену складність та брак обчислювальної потужності. У машинному навчанні використовуються математичні методи для прогнозування або класифікації даних без необхідності програмувати правила та попередні знання людини. Початкові підходи машинного навчання розроблені для вирішення простих лінійних проблем. У наступні десятиліття розроблені штучні нейронні мережі, які функціонували в каскаді з кількох процесорів і забезпечували можливість розв’язувати дуже

складні нелінійні проблеми. Розвиток машинного навчання протягом століття значно зріс після появи інтернету, що привело до сучасних хмарних систем. Подальше зростання спричинене розробкою графічних процесорів, створених для ігрової індустрії. Ці процесори здатні значно покращити паралельну обробку великих обсягів даних, що дозволяє навчати надзвичайно складні моделі з великими обсягами даних. У наш час університети США, Нідерландів, Китаю, Японії та інших країн активно займаються розробкою програм та створенням медичних закладів, які оснащені ШІ. Застосування ШІ у медицині вперше описано в 1976 р., коли використано комп'ютерний алгоритм для виявлення причин гострого болю в животі. ШІ дає можливість виявити такі захворювання, як рак шкіри, діабетична ретинопатія; при вдосконаленні класифікації патології, наприклад, описі сканованих зображень у радіології або особливостей електрокардіограми (ЕКГ); у прогнозуванні моделей захворювань, яскравим прикладом чого є алгоритми на основі МН, розроблені під час пандемії COVID-19. Бездротові або безконтактні технології є особливо важливими під час пандемії COVID-19, оскільки потребують найменшого контакту інфікованих хворих і медичних працівників. Технологія радіочастотного зондування здатна збирати інформацію з тіла пацієнта. Передача цієї інформації через алгоритми ШІ дає цінні результати без будь-якої прямої участі медичних працівників. Технології віддаленого безконтактного зондування, інтегровані з інтелектуальними алгоритмами машинного навчання, здатні давати правильні результати в режимі реального часу, що може бути легко використано клініцистом для моніторингу та діагностики захворювання, а саме симптомів COVID-19, наприклад порушень дихання у вигляді задишки та ін.» [5].

Штучний інтелект в медицині може проявлятися в різних аспектах, зокрема:

- розвивати наукові дослідження в сфері медицини. Вовк А.В. вказує, що «системи штучного інтелекту можуть збирати і структурувати інформацію про повну історію хвороби, лабораторні дані під час лікування і стан організму в певний момент часу. Дані, завантажені в базу даних, ретельно обробляються електронними мізками для швидкого аналізу. Це прискорює процес прийняття рішень медичним персоналом і сприяє більш точному діагнозу та своєчасному призначенню необхідного лікування. Наприклад, так працює система Watson Health System від IBM. Виявляючи потенційні проблеми в судинній системі, розпізнаючи рак і визначаючи, чи схильний пацієнт до утворення тромбів, IBM Watson може швидко реагувати на необхідність аналізу нової інформації і робити на її основі висновки. Наприклад, штучний інтелект IBM може проаналізувати 20 мільйонів наукових робіт з онкології за 10 хвилин і поставити правильний діагноз пацієнту» [6]. «Великі мовні моделі штучного інтелекту мають потенціал значно сприяти медичній галузі, зокрема у плані обробки великих обсягів медичних даних та підтримки прийняття клінічних рішень. Ці технології можуть відігравати ключову роль у зборі, аналізі та інтерпретації медичної інформації, необхідної для розробки індивідуалізованих лікувальних планів. Наприклад, аналіз генетичних даних пацієнтів із застосуванням штучного інтелекту може сприяти виявленню ризиків розвитку захворювань на ранній стадії та формуванню ефективних стратегій профілактики та лікування.» [30]. Це вказує, що технології штучного інтелекту дозволяють пришвидшувати процеси наукових досліджень щодо пошуку нових методів лікування;

- удосконалювати процеси діагностики, лікування та реабілітації. «За результатами досліджень було виявлено, що штучний інтелект, який почав своє існування ще в 1950 роках минулого століття, здійснив значний прорив у сфері медицини. ШІ використовує складні алгоритми машинного навчання для обробки великої кількості даних, навчання та згодом –

створення корисного результату для вирішення чітко визначеної проблеми в медичній системі. Навчившись, системи штучного інтелекту можуть звільнити час зайнятим лікарям, переписуючи нотатки, вводячи та впорядковуючи дані пацієнтів, персоналізувати лікування, надавати дистанційно діагностику пацієнтам, відповідаючи на їх основні запитання та надсилати необхідні ресурси. Але найголовніше, що такі системи ШІ є точними, дозволяють розроблювати ліки, допомагають проводити операції та можуть заздалегідь більш ефективніше діагностувати небезпечне захворювання у пацієнта ще на ранній його стадії і тим самим врятувати життя людини» [33]. Варто наголосити, що необхідно розрізняти використання технологій штучного інтелекту при лікуванні лікарем та технологій штучного інтелекту, на основі яких працюють медичні технології.

- підвищення ефективності управління закладами охорони здоров'я. Впровадження штучного інтелекту в систему державного управління та роботу клінік суттєво підвищує ефективність закладу за рахунок автоматизації рутинних процесових завдань та інтелектуальної обробки даних. На управлінському рівні алгоритми штучного інтелекту дозволяють точніше прогнозувати потоки пацієнтів, оптимізувати закупівлі медикаментів і раціонально розподіляти робочий час персоналу. Водночас законодавче врегулювання ШІ за стандартами ЄС (AI Act) гарантує прозорість, безпеку та високу точність таких рішень під постійним контролем лікаря (Human-in-the-loop).

- підвищення доступності та якості медичних послуг. «Останніми десятиліттями значно підвищився інтерес до застосування штучного інтелекту (ШІ) у сфері охорони здоров'я, який змінює парадигму завдяки зростанню доступності медичних даних і швидкому прогресу аналітичних методів. Його можна застосовувати для різних типів медичних даних - структурованих і

неструктурованих. Популярні методи ШІ включають методи машинного навчання (МН) для структурованих даних, такі як класична машина опорних векторів і нейронна мережа, сучасне глибоке навчання, а також обробку неструктурованих даних. До основних галузей медицини, де застосовують інструменти ШІ, належать онкологія, неврологія, кардіологія, ендокринологія, стоматологія та ін.. Найбільші світові ІТ-компанії, серед них Microsoft, IBM, Intel, Google та ін., мають власні розробки на основі ШІ, які допомагають вирішувати подібні задачі. Наприклад, IBM Watson - суперкомп'ютер фірми IBM, оснащений системою ШІ, створений групою дослідників під керівництвом Девіда Феруччі, використовують для допомоги у прийнятті управлінських рішень при лікуванні хворих на рак легень» [5].

Зазначене забезпечується тим, що сучасні технології вже використовуються в різних видах медичної допомоги, зокрема:

- діагностика. «Виробники медичного обладнання активно досліджують та розробляють програми, за допомогою яких ШІ аналізує зображення з комп'ютерної томографії (КТ), для вдосконалення КТ-зображень, а також для лабораторних аналізів крові, збору даних з вимірювачів артеріального тиску, електрокардіографів та інших пристроїв, навіть вивчення ДНК пацієнтів, щоб підібрати найбільш коректні методи лікування» [5];

- офтальмологія. «В офтальмології ШІ застосовують для підтвердження діагнозу захворювань, читання зображень, виконання топографічного картування рогівки та розрахунків інтраокулярних лінз. Офтальмологічна візуалізація забезпечує спосіб діагностики та об'єктивного виявлення прогресування низки хвороб, яка включає діабетичну ретинопатію, вікову дегенерацію жовтої плями, глаукому та інші офтальмологічні розлади. У якості діагностичних методів в офтальмологічній практиці використовують два методи візуалізації:

цифрову фотографію очного дна та оптичну когерентну томографію. Очікується, що найближчим часом разом ШІ і МН нададуть офтальмологам автоматизовані пристрої для ранньої діагностики та своєчасного лікування захворювань цього профілю» [5];

- кардіологія. «Впровадження в клінічну практику ШІ при серцевосудинних захворюваннях поступово набирає обертів і, як очікується, зрештою охопить увесь спектр стратифікації ризику, діагностики, лікування та прогнозу. Алгоритми класифікації вже застосовані в кількох пакетах програмного забезпечення для попередньої обробки ехокардіографічних зображень (сегментація зображення). Наприклад, камери серця можна окреслити автоматично і розрахувати такі значення, як фракція викиду або вимірювання поздовжньої деформації. Розроблена також сегментація на основі КТ і магнітно-резонансної томографії серця, запропонована можливість прогнозувати результати візуалізації перфузії міокарда позитронно-емісійною томографією на основі інтеграції простих даних. Це свідчить про те, що відбір пацієнтів для направлення на спеціалізовану та вартісну візуалізацію можна оптимізувати за допомогою ШІ. Нещодавно метод МН застосований для інтеграції генетичної та клінічної інформації для покращення прогнозування ішемічної хвороби серця порівняно зі звичайними факторами ризику» [5];

- ортопедія. «Оцінено та кількісно визначено викривлення хребта при сколіозі, а також розроблено алгоритми, здатні обчислювати кут Кобба за допомогою топографії поверхні перед використанням рентгенограм і тривимірних зображень. Згодом ШІ використали для виявлення інших видів патології хребта, наприклад кили диска або переломів хребців. Крім того, використання сегментації зображення в реальному часі використовують як інструмент навігації в хірургії хребта. Нещодавно

сфера застосування ШІ для допомоги в діагностичній візуалізації розширилася за межі хребта, починаючи з ідентифікації переломів стегна до розривів меніска м'яких тканин у коліні. Відбувся також перехід до алгоритмів, що забезпечують детальнішу оцінку захворювання. Подальший розвиток ШІ в ортопедії сприятиме підвищенню точності та зручності у стратифікації ризиків, прийнятті клінічних рішень, підтримці та розширенні роботизованої хірургії» [5].

Штучний інтелект стає невід'ємним елементом сучасної системи охорони здоров'я, охоплюючи наукові дослідження, діагностику, лікування, реабілітацію та управління закладами охорони здоров'я. Водночас його широке впровадження породжує нові ризики, пов'язані із безпекою, етикою, захистом медичних даних, відповідальністю та якістю медичної допомоги.

Зазначене характеризує потребу у впровадженні технологій штучного інтелекту в системі охорони здоров'я, адже неврегульованість даного питання може призвести до сукупності проблем, зокрема:

- спотворення результатів наукових досліджень через порушення принципів академічної доброчесності вченими-медиками;

- лікарських помилок через неетичне використання технологій штучного інтелекту;

- забезпечення приватності та захисту медичних персональних даних як лікарів, так і пацієнтів;

- використання штучного інтелекту без відповідної підготовки, що може призвести до лікарських помилок.

Вітчизняні дослідники А.П. Колесніков та О.М. Карапетян [20] визначають ключові аспекти, пов'язані з законодавчим регулюванням штучного інтелекту в Україні:

«- приватність та захист даних: У зв'язку з використанням штучного інтелекту, який обробляє великі обсяги даних, виникають питання щодо

приватності та захисту персональних даних. Закон України «Про захист персональних даних» забезпечує певні заходи забезпечення конфіденційності та захисту персональних даних, але деякі аспекти, пов'язані з обробкою даних штучним інтелектом, можуть вимагати додаткового регулювання. Зокрема, у визначенні термінів (стаття 2) доцільно уточнити термін «третя особа» і його трактування. У випадку допуску штучного інтелекту до обробки персональних даних він буде виступати у ролі «третьої сторони» (пропонуємо саме таке трактування, оскільки наразі штучний інтелект не можна вважати «особою», навіть віртуальною), тому є необхідним коригування даного положення статті Закону, і аналогічних положень у інших законодавчих актах;

- етика та безпека штучного інтелекту. Розвиток штучного інтелекту також поставив питання етичності та безпеки. Законодавці в Україні можуть вивчати можливості встановлення стандартів і норм поведінки, які забезпечать етичне використання штучного інтелекту;

- штучний інтелект у сферах використання. У різних галузях, таких як медицина, транспорт, фінанси, юстиція, можуть бути потрібні спеціальні нормативні акти, що регулюють використання штучного інтелекту в конкретних сферах. Наприклад, для автономних транспортних засобів або медичних діагностичних систем;

- заохочення досліджень та інновацій. Розвиток штучного інтелекту в Україні може потребувати створення сприятливих умов для досліджень та інновацій, таких як надання грантів, підтримка стартапів, сприяння співпраці між академічними установами та промисловими компаніями» [20].

У зв'язку з цим державне регулювання використання ШІ в охороні здоров'я має формувати комплексну систему правових, організаційних та інституційних механізмів, спрямованих одночасно на забезпечення безпеки

пацієнтів і медичних працівників, захист персональних даних, дотримання етичних принципів та створення умов для розвитку інновацій. Водночас аналіз праць зарубіжних учених показує, що питання державного регулювання ШІ в медицині потребує подальшого системного дослідження, зокрема з позицій формування ефективної моделі державного управління та адаптації європейських регуляторних підходів до національної системи охорони здоров'я.

Аналізуючи праці зарубіжних вчених, сьогодні можна виділити ключові проблеми державно-управлінського характеру, що пов'язані із використанням технологій штучного інтелекту в системі охорони здоров'я (табл. 5.3).

Таблиця 5.3

Державно-управлінський характер проблем впровадження технологій штучного інтелекту в медицині

Проблема	**Характеристика**	**Джерело**
1	*2*	*3*
Проблеми державного регулювання		
Дефіцит юридичної визначеності щодо суб'єкта цивільно-правової відповідальності за медичні помилки	- розрив між нормативним статусом лікаря як єдиного класичного суб'єкта відповідальності та відсутністю правових механізмів притягнення до відповідальності розробників алгоритмів ШІ у разі заподіяння шкоди пацієнту	Gerke, S., Minssen T., Cohen G. [160]
Неадекватність регуляторних процедур сертифікації щодо алгоритмів безперервного самонавчання	- традиційний правовий режим допуску медичних виробів вимагає фіксованого коду, що створює нормативний вакуум при оцінці відповідності систем ШІ, які змінюють свою логіку в реальному часі на нових даних	Vokinger, K.N., Feuerriegel S., Kesselheim A.S. [273]
Відсутність нормативних механізмів правового захисту пацієнтів від алгоритмічної дискримінації	- недосконалість антидискримінаційного законодавства у сфері eHealth, яке не містить норм щодо правового аудиту медичних алгоритмів, що поглиблюють нерівність у доступі до якісної медичної допомоги	Hussain S.A., Bresnahan M., Zhuang J. [176]

Продовження табл. 5.3

1	*2*	*3*
Відсутність обов'язкових нормативних стандартів попередньої валідації та аудиту навчальних датасетів	- законодавча незахищеність споживачів медичних послуг через відсутність нормативно закріпленого обов'язку розробників перевіряти вхідні дані на наявність упереджень до моменту реєстрації ШІ-продукту	Ratwani R.M., Sutton K., Galarraga J.E. [237]
Прихована системно-алгоритмічна упередженість у комерційних ШІ-системах	- юридично некоректна зміна цільових метрик у коді, коли правова концепція «потреби пацієнта в медичній допомозі» (зокрема пацієнтів різних рас) підміняється математичним показником «попередніх фінансових витрат на пацієнта», що порушує принцип рівності	Obermeyer Z., Powers B., Vogeli C., Mullainathan S. [223]
Законодавчий конфлікт між вимогами захисту приватних даних та створенням репрезентативних навчальних вибірок	- колізія між правовим режимом суворого обмеження обробки чутливих медичних даних і технічною потребою ШІ в наданні репрезентативних масивів для запобігання похибкам	Chen I.Y., Pierson E., Rose S. та інші [120]
Проблеми економічних механізмів		
Відсутність державних та страхових моделей компенсації витрат за застосування ШІ	- традиційні механізми фінансування медичної допомоги переважно орієнтовані на оплату медичних послуг та процедур, тоді як внесок програмних AI-систем у діагностику, прийняття клінічних рішень, моніторинг пацієнтів або управління ресурсами складно відокремити та оцінити в межах існуючих моделей оплати	Davenport T., Kalakota R. [129]
Економічна неефективність через невраховані приховані витрати на підготовку даних	- систематичне ігнорування у кошторисах значних фінансових та часових витрат на залучення висикооплачуваних медичних фахівців для структурування, анонімізації та маркування первинних даних	Sendak M.P., D'Arcy J., Kashyap S. та інші [254]
Відсутність окремих тарифно-компенсаційних кодів для ШІ-послуг	- страхові компанії та державні програми не мають стандартизованих тарифів для відшкодування вартості роботи ШІ. Лікарні змушені купувати ШІ за власні кошти, не маючи змоги законно виставити рахунок пацієнту чи страховику, що робить ШІ економічно збитковим	Kazi D.S., Lu R., Wadhera R. K. [108]
Високі постійні витрати на кібербезпеку, оновлення та підтримку обладнання	- придбання ШІ-софту є лише часткою витрат, в той час як основне фінансове навантаження припадає на придбання потужних графічних процесорів, їх охолодження, оплата праці спеціалістів із кібербезпеки та регулярна перевалідація моделей. Малі клініки не мають економічного масштабу, щоб розподілити ці фіксовані витрати на велику кількість пацієнтів	Bertalan Meskó, Marton Görög [215]

Продовження табл. 5.3

1	*2*	*3*
Поглиблення економічного та технологічного розриву між суб'єктами господарювання в медицині	- висока вартість інфраструктури та підтримки ШІ створює фінансовий бар'єр, який формує монополію багатих приватних центрів і знецінює ресурсну спроможність державних закладів	Bajwa J.S., Munir U., Nori A., Williams B. [102]
Проблеми управління та організації		
Управлінський ризик, спричинений відсутністю інтрепретації принципів прийняття рішень алгоритмами	- нездатність ШІ пояснити логіку отриманого клінічного результату створює кризу довіри та блокує прийняття управлінських і медичних рішень керівниками та лікарями	Topol, E.J. [266]
Організаційна деградація професійних компетенцій медичного персоналу	- психологічна та операційна залежність лікарів від підказок ШІ, яка у довгостроковій перспективі призводить до втрати базових навичок самостійного клінічного мислення	Cabitza F., Rasoini R., Gensini G. F. [114]
Проблеми управління та організації		
Зсув управлінського фокусу та дегуманізація операційного процесу надання медичної допомоги	- нераціональний розподіл робочого часу лікаря, коли взаємодія з цифровими інтерфейсами та введення даних переважає над безпосереднім контактом з пацієнтом	Verghese A., Shah N.H., Harrington R.A. [268]
Інтеграційний розрив між лабораторною точністю ШІ та реальним клінічним процес-менеджментом	- провал високоефективних в ізольованому середовищі алгоритмів під час спроби їх впровадження у складні, нестандартизовані та хаотичні операційні процедури лікарні	Panch T., Mattie H., Celi L.A. [232]
Низький рівень техніко-організаційної сумісності та психологічний опір персоналу	- технологічна застарілість наявних Медичних інформаційних систем (МІС) у поєднанні з відсутністю системного кадрового менеджменту щодо подолання заперечення технологій з боку лікарів	Kelly C.J., Karthikesalingam A., Suleyman M. та інші [185]

Переважна більшість із цих проблем (понад 85 %) залишаються актуальними сьогодні, однак у світовій та європейській практиці з'явилися перші нормативні інструменти для їх часткового вирішення. Адже попри стрімкий технологічний прогрес самого ШІ, державне управління, економічні моделі фінансування та організаційна структура медичних закладів адаптуються значно повільніше, створюючи суттєвий гальмівний ефект. Ефективне впровадження ШІ в охорону здоров'я вимагає від держави переходу від концепції суто технологічного імпорту до побудови

комплексного механізму державного управління, який одночасно охоплюватиме адаптивне правове регулювання, нові страхово-економічні стимули та продуманий кадрово-організаційний менеджмент.

Зазначені проблеми є характерними і для України, саме тому є потреба в розробці механізмів державного регулювання використання штучного інтелекту в медицині. Розробка механізму має врахувати сукупність факторів, зокрема:

- політико-правових, що визначаються євроінтеграційними процесами, а отже система державного регулювання має бути адаптована до директив, регламентів та інших нормативних актів Європейського Союзу і в той же час забезпечити врахування національних інтересів, які можуть видозмінюватися на різних етапах розвитку;

- соціально-економічних, що обумовлені економічними та соціальними наслідками російсько-української війни, а отже вплинули на дефіцит бюджету, а отже обмежене фінансування системи охорони здоров'я і як наслідок неможливість модернізації цифрової інфраструктури для забезпечення її безпеки;

- ментально-культурних, що визначаються впливом культурних, релігійних факторів та системи цінностей на сприйняття суспільством інноваційних технологій в цілому та штучного інтелекту зокрема, адже це може спричинити спротив окремих осіб щодо використання штучного інтелекту при отриманні медичних послуг;

Відповідно розробка та впровадження механізмів державного регулювання впровадження технологій штучного інтелекту у функціонування системи охорони здоров'я має врахувати усі зазначені фактори.

У Європейському Союзі питання регулювання технологій штучного інтелекту регулюються сукупністю нормативно-правових актів, зокрема:

- Регламент (ЄС) 2024/1689 про штучний інтелект (AI Act). Документ є першим у світі всеохоплювальним горизонтальним законом, який законодавчо закріплює ризик-орієнтований підхід до класифікації цифрових продуктів. Більшість медичних ШІ-систем (зокрема діагностичний софт, алгоритми прийняття клінічних рішень та автономне хірургічне обладнання) офіційно віднесено до категорії регулювання високого ризику (High-Risk AI Systems). Для виходу на ринок розробники зобов’язані впровадити комплексну систему управління ризиками, довести високу якість навчальних датасетів та забезпечити наскрізну прозорість дій алгоритму. Законами ЄС встановлено жорстку вимогу щодо обов'язкового постійного людського нагляду (Human-in-the-Loop), що забороняє повну автономність алгоритмів у критичних медичних ситуаціях. Окрім того, регламент запроваджує постійний постринковий моніторинг та передбачає астрономічні штрафи за вихід на ринок некоректно валідованих моделей.

-- Директива (ЄС) 2024/2853 про відповідальність за дефектну продукцію (PLD). Нормативний акт докорінно модернізує правовий режим цивільної відповідальності ЄС, пристосовуючи його до умов цифрової епохи та економіки даних. Директива офіційно розширює юридичне визначення поняття «продукт», вперше включаючи до нього програмне забезпечення, автономні алгоритми та цифрові файли медичного призначення. Ключовою новелою є суттєве спрощення процесуального тягаря доведення вини для пацієнтів у разі заподіяння шкоди їхньому здоров'ю через медичну помилку ШІ. Якщо позивач доводить технічну складність або «закритість» алгоритму, суд має право застосувати презумпцію дефектності продукту або причинно-наслідкового зв'язку. Це змушує розробників та медичні заклади завчасно дбати про страхування відповідальності й повну документованість роботи алгоритмів.

Крім зазначених актів важливе значення у врегулюванні питань використання штучного інтелекту в медицині мають стратегічні та рамкові документи Європейського Союзу, зокрема:

- Етичні настанови щодо надійного ШІ (Ethics Guidelines for Trustworthy AI, 2019) [150] - це фундаментальний рамковий документ, розроблений Експертною групою високого рівня з питань ШІ (HLEG) при Європейській Комісії, який заклав ідеологічну та концептуальну основу для всього подальшого законодавства ЄС. Аналізуючи документ, варто наголосити на сукупності обов’язкових вимог до систем штучного інтелекту (табл. 5.4).

Таблиця 5.4

Ключові вимоги до технологій штучного інтелекту, що визначені Етичними настановами щодо надійного ШІ (Ethics Guidelines for Trustworthy AI) [150]

Вимога	Характеристика
Людський контроль та нагляд	системи мають підтримувати людську автономність і підпорядковуватися обов'язковому людському нагляду
Технічна міцність та безпека	алгоритми мусять бути стійкими до збоїв, захищеними від кібератак і гарантувати точність та відтворюваність результатів
Приватність та управління даними	забезпечення повного захисту чутливих даних пацієнтів/користувачів і належної якості навчальних вибірок
Прозорість	алгоритми, дані та бізнес-моделі мають бути пояснюваними, а користувачі повинні завжди знати, що вони взаємодіють із ШІ
Різноманітність, недискримінація та справедливість	обов'язкове усунення системних упереджень (*bias*) у датасетах для запобігання алгоритмічній дискримінації окремих груп населення
Суспільне та екологічне благо	ШІ повинен використовуватися для сталого розвитку, підвищення якості життя та без шкоди для довкілля
Підзвітність	впровадження механізмів аудиту, оцінки ризиків до виходу продукту на ринок та забезпечення можливості відшкодування завданих збитків

- Біла книга про штучний інтелект (White Paper on AI, 2020) [277] - це стратегічний концептуальний документ, оприлюднений Європейською Комісією 19 лютого 2020 року. Центральна ідея Білої книги - Європа має стати світовим лідером у сфері ШІ, побудувавши унікальний підхід, який поєднує підтримку інновацій із захистом фундаментальних прав людини та європейських цінностей. Зазначений документ визначає формування двох взаємопов’язаних екосистем (табл. 5.5).

Таблиця 5.5

Характеристика Білої книги ЄС про штучний інтелект [277]

Екосистеми	Мета	Ключові напрями
Екосистема досконалості	залучення інвестицій, розвиток досліджень та підтримка бізнесу (особливо стартапів та малого/середнього бізнесу)	Мобілізація понад €20 млрд щороку на дослідження та розгортання ШІ через програми Horizon Europe та Digital Europe; створення національних Центрів цифрових інновацій; розширення доступу до промислових і публічних даних
Екосистема довіри	створення чіткої та передбачуваної нормативно-правової бази, яка гарантує безпеку громадян і застереже від порушення їхніх прав	Започаткування ризик-орієнтованого підходу (Risk-based approach). Регулювання має стосуватися перш за все систем штучного інтелекту з високим ризиком.

Аналізуючи національне законодавство, варто наголосити, що в Україні реалізовані окремі положення, які стосуються зазначених стратегічних та рамкових документів, а саме:

- Концепція розвитку штучного інтелекту в Україні, яка затверджена Розпорядженням Кабінету Міністрів України № 1555-р від 2 грудня 2020 року [55] та визначає пріоритетні сфери застосування ШІ (зокрема медицину) та прямо посилається на принципи Європейського Союзу щодо безпечного, етичного та людиноцентричного ШІ.

- Дорожня карта з регулювання штучного інтелекту в Україні (2023–2026) [62] - поетапний план гармонізації українського законодавства із законодавством ЄС. Перший етап передбачав добровільні етичні кодекси та інструменти самооцінки (аналоги європейського ALTAI), а підсумковий етап має забезпечити імплементацію норм EU AI Act у національне законодавство України.

- Добровільний кодекс поведінки для українських компаній, які створюють та інтегрують алгоритми ШІ [29], зокрема у сфері HealthTech та діагностики.

- Рекомендації з відповідального використання штучного інтелекту [29] - методичні рекомендації для бізнесу та розробників, які засновані на 7 етичних принципах HLEG ЄС: прозорості, недискримінації, безпеці, підзвітності та обов'язковому людському контролі.

Зазначене має лягти в комплексний механізм державного регулювання використання технологій штучного інтелекту у функціонуванні системи охорони здоров’я (табл. 5.6).

Прийняття Рамкового закону України «Про штучний інтелект» покликане створити чітке, прозоре та безпечне правове поле для розробки й інтеграції передових цифрових технологій, узгоджене із стандартами Європейського Союзу. Це забезпечить формування цілісної правової та інституційної основи державного регулювання розроблення, впровадження і використання технологій штучного інтелекту на засадах безпеки, прозорості, підзвітності, захисту прав людини та ризик-орієнтованого підходу. Потреба в його прийнятті обумовлена поширенням технологій ШІ у суспільно значущих сферах, зокрема в охороні здоров’я, та необхідністю комплексного врегулювання ризиків і відносин, які не охоплюються повною мірою чинним законодавством.

Закон вирішує завдання чіткої категоризації ШІ-систем за рівнями ризику та встановлення суворих вимог до безпеки, прозорості й обов’язкового людського контролю алгоритмів. Крім того, він нормує розподіл цивільно-правової відповідальності між розробниками, постачальниками та користувачами, створюючи ефективні механізми відшкодування потенційної шкоди. Окремими завданнями є формування економічних механізмів розвитку ШІ, забезпечення міжвідомчої взаємодії та міжнародного співробітництва, а також встановлення особливостей державного регулювання використання ШІ в окремих сферах, передусім у системі охорони здоров’я.

Таблиця 5.6

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. 5.6

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 11. 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. 5.6

Розділ 12. 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 13. 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 14. 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 АКТІВ			
- прийняття Постанови КМУ про затвердження 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	

Ухвалення документа докорінно змінить підхід до впровадження інновацій, перевівши стихійне застосування алгоритмів у контрольований, підзвітний та юридично захищений формат. Для цифровізації системи охорони здоров'я Закон сформує правові, інституційні, організаційні та економічні передумови безпечного впровадження ШІ в діагностику, лікування, наукові дослідження та управлінські процеси із забезпеченням захисту прав пацієнтів, медичних даних і належного людського контролю.

Прийняття Закону України «Про штучний інтелект» зумовлює сукупність змін в Законі України «Основи законодавства України про охорону здоров'я», зокрема:

- доповнити Статтю 3 новими термінами: медична система штучного інтелекту (система штучного інтелекту або її окремий алгоритм, що використовується самостійно або як складова частина медичного виробу для діагностики, профілактики, моніторингу, прогнозування перебігу захворювань чи підтримки прийняття клінічних рішень); система підтримки прийняття клінічних рішень на основі штучного інтелекту (програмна система, що аналізує медичні дані пацієнта та надає медичному працівнику інформаційно-аналітичні рекомендації щодо діагностики або лікування, залишаючи остаточне рішення за лікарем);

- Доповнити статтею 35-7: Стаття 35-7. Застосування технологій штучного інтелекту в медичній практиці, що передбачає наступне формулювання: «а) Технології штучного інтелекту застосовуються в медичній практиці виключно як допоміжний інструмент для підтримки клінічних рішень, наукових досліджень, аналізу медичних даних або автоматизації адміністративних процесів; б) Принцип збереження людського контролю (Human-in-the-Loop): Забороняється прийняття остаточних юридично значущих діагностичних чи лікувальних рішень щодо пацієнта виключно в автоматичному режимі за допомогою медичних систем штучного інтелекту. Остаточне рішення про встановлення діагнозу, призначення чи скасування

лікування приймає виключно медичний працівник; в) До застосування в медичній практиці допускаються лише медичні системи штучного інтелекту високого ризику, які пройшли процедуру оцінки відповідності, отримали Декларацію відповідності та внесені до Державного реєстру систем штучного інтелекту високого ризику та Державного реєстру медичних виробів»;

- доповнити статтю 39 новою частиною: «У разі використання медичної системи штучного інтелекту під час надання медичної допомоги лікар зобов'язаний поінформувати про це пацієнта (або його законного представника) в доступній формі, а також роз'яснити мету та особливості використання такої системи. Інформація про застосування штучного інтелекту підлягає обов'язковій фіксації в електронній системі охорони здоров’я»;

- доповнити статтю 39-1 новою частиною такого змісту: «Пацієнт має право на отримання інформації про логіку прийняття рекомендацій медичною системою штучного інтелекту, що була використана під час його діагностики чи лікування, а також право вимагати перегляду відповідного рішення безпосередньо медичним працівником (лікарем)»;

- доповнити Статтю 77 новою частиною: «Медичні працівники не несуть цивільно-правової відповідальності за шкоду, завдану здоров'ю пацієнта, якщо така шкода була спричинена прихованим дефектом, збоєм або недосконалістю алгоритму медичної системи штучного інтелекту, за умови, що лікар дотримався встановлених клінічних протоколів, інструкцій з експлуатації системи та реалізував належний професійний контроль»;

- доповнити статтю 78 новою частиною такого змісту: «Медичні та фармацевтичні працівники зобов'язані володіти базовими цифровими компетенціями щодо безпечного та відповідального використання систем штучного інтелекту в межах своєї професійної діяльності, регулярно проходити підвищення кваліфікації з питань цифрової медицини».

Потреба у прийнятті нових та внесенні змін до чинних підзаконних нормативно-правових актів зумовлена необхідністю практичної реалізації положень рамкового Закону про штучний інтелект та встановлення спеціальних процедур використання ШІ у сфері охорони здоров'я. Метою є нормативне врегулювання процедур допуску, інтеграції, використання та постринкового моніторингу медичних систем ШІ, а також вимог до медичних даних і захисту прав пацієнтів. Основними завданнями є встановлення порядку підключення та верифікації ШІ-модулів в електронній системі охорони здоров'я, запровадження постійного моніторингу та повторної оцінки систем ШІ, визначення вимог до використання ШІ як медичного виробу, стандартизація підготовки медичних даних для навчання і тестування алгоритмів та нормативне закріплення інформування пацієнтів про застосування ШІ. Це дозволить перевести загальні положення законодавства про ШІ у конкретні регуляторні процедури та сформувати єдині правила безпечного впровадження, використання, контролю й моніторингу технологій ШІ в системі охорони здоров'я.

Таким чином, 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. 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.

У результаті 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. 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.

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 штучного інтелекту в цифрову систему охорони здоров'я 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 Європейського Союзу. У ширшому контексті це дозволяє розглядати державне регулювання ШІ не як окремий напрям цифрової політики, а як складову державного управління цифровою трансформацією системи охорони здоров'я, від ефективності якої залежатимуть якість, доступність, безпека та інноваційність медичної допомоги.

5.3. Механізми розширення інституційної спроможності державного управління цифровою трансформацією системи охорони здоров'я

Цифрова трансформація системи охорони здоров'я, будучи складним об'єктом державного управління, вимагає розширення інституційної спроможності, що зумовлено сукупністю вимог євроінтеграційних процесів, що стосуються управління даними, захисту персональних даних, використання штучного інтелекту та інше. Розширення інституційної спроможності полягає в потребі утворення нових суб'єктів державного управління, розширення повноважень існуючих, що дозволить вирішити сукупність проблем організаційного, інформаційного, регуляторного, наглядового, контрольного та комунікаційного характеру. Варто зазначити, що інституційне розширення стосується не стільки системи охорони здоров'я, скільки політики цифрової трансформації загалом.

Зазначені питання частково розкриті в працях зарубіжних вчених, зокрема в частині реалізації положень директив та регламентів Європейського Союзу: 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), Джонатан Стокс (Jonathan Stokes), 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), Бастіан Гаук (Bastian Hauck), Мішель Пенже (Michel Pinget), Майк Ліпс (Mike Leers), Тар'я Стенвалл (Tarja Stenvall), Нік Гюлдемонд (Nick Guldemond), Луція Мокра (Lucia Mokrá) та інші. Серед зарубіжних вчених питання розвитку суб’єктної складової державного управління системою охорони здоров’я: Д.О. Грицишен, Л.В. Сергієнко, Л.В. Антонова, С.М. Петрик, А.А. Висоцький, О.О. Суріков, С.В. Василюк-Зайцева, В.В. Мельник, В.В. Кривецький, Д.В. Проняєв, М.С. Саєнко, А.В. Вовк, М.І. Мойсеєнко, М.М. Кузишин, Л.В. Туровська, Ю.С. Мазуренко, М.Л. Петришин, О.І. Пархоменко-Куцевіл та інші.

Розширення інституційної спроможності - це процес посилення здатності суб’єктів державного управління, закладів охорони здоров’я або будь-якої іншої організації ефективно виконувати свої функції, реалізовувати стратегічні цілі та адаптуватися до нових викликів цифрової трансформації в умовах євроінтеграції.

Зважаючи на комплекс визначених проблем цифрової трансформації в попередніх дослідженнях, пропонуємо наступний комплексний механізм розширення інституційної спроможності державного управління цифровою трансформацією системи охорони здоров'я (табл. 5.7).

Комплексний механізм розширення інституційної спроможності державного управління цифровою трансформацією системи охорони здоров'я має охопити сукупність напрямів, зокрема:

1. Розширення інституційної спроможності для забезпечення безпечного вторинного використання медичних даних (health data access body (орган з доступу до медичних даних)). Даний напрямок може відбуватися двома шляхами: 1) утворення нового суб'єкту державного управління - Національного агентства з доступу до медичних даних (HDAB Ukraine); 2) наділення відповідними повноваженнями існуючого суб'єкту. Незалежно від обраного варіанту на дану інституцію покладатимуться наступні завдання:

- видача дозволів на доступ до даних;
- забезпечення анонімізації та псевдонімізації;
- управління безпечними середовищами обробки;
- контроль вивантаження результатів;
- адміністрування реєстру відмов пацієнтів;
- забезпечення інтеграції в єдину мережу HealthData@EU;
- прийняття участі в наукових дослідженнях;
- регуляторна діяльність щодо суб'єктів медичних даних.

Варто зазначити, що в країнах Європейського Союзу відповідність регламенту (ЄС) 2025/327 про Європейський простір медичних даних також відбувалася різними шляхами, що представлено в таблиці 5.8.

Таблиця 5.7

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 повноваженнями 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 для забезпечення безпечного вторинного використання медичних даних</td><td colspan="2">- наділення повноваженнями та формування структурного підрозділу в структурі Міністерства охорони здоров'я України</td></tr>
<tr><td colspan="2">- наділення повноваженнями 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 colspan="2">Інформаційно-інфраструктурне забезпечення</td><td>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 colspan="2">- побудова вузла взаємодії (NCPH Node);
- впровадження єдиного формату EEHRxF;
- гармонізація медичних кодифікаторів</td><td>- внесення змін до Постанови КМУ Про затвердження Порядку функціонування ЕСОЗ
- розробка Порядку транскордонного обміну медичними даними;
- угода про приєднання до мережі MyHealth@EU</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 виступатиме 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. 5.7

<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 агентства 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 проводити аудит алгоритмів 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>

Таблиця 5.8

Особливості формування органу з доступу до медичних даних (health data access body) в країнах-членах Європейського Союзу

Країна	Суб'єкт	Характеристика
Фінляндія	*Спеціалізований існуючий орган*	- створено Findata — Finnish Social and Health Data Permit Authority, що видає дозволи на вторинне використання даних, збирає та об'єднує дані, здійснює їх попередню обробку та забезпечує захищене середовище Kapseli для аналізу, що адаптовано до EHDS
Данія	*HDAB на базі існуючої інституційної системи*	- Danish Health Data Authority реалізує проєкт HDAB Denmark: формується національний каталог метаданих, створюється портал подання заявок на доступ, який надалі буде пов'язаний з каталогами інших держав ЄС
Франція	*Використання сформованої інфраструктури медичних даних*	- Франція вже має Health Data Hub (Plateforme des données de santé) та національну систему медичних даних SNDS
Німеччина	*Розподілена інституційна модель із централізацією доступу*	- німецька модель розвивається навколо національної інфраструктури доступу до медичних даних та Forschungsdatenzentrum Gesundheit; у процесі адаптації до EHDS обговорюється центральна координаційна функція доступу до медичних даних

Щодо України, то за умови утворення нового суб'єкту державного управління - Національного агентства з доступу до медичних даних (HDAB Ukraine), пропонуємо визначати його як орган центральної виконавчої влади, що наділений відповідними повноваженнями та має повну функціональну незалежність та автономність прийняття рішень для забезпечення безпечного вторинного використання медичних даних.

Національне агентство з доступу до медичних даних має володіти сукупністю повноважень дозвільного, контрольного, інформаційно-аналітичного, технічного, координаційного та регуляторного характеру, що закріплено в Регламенті (ЄС) 2025/327 про Європейський простір медичних даних. До його компетенції мають належати прийняття рішень про надання доступу до медичних даних, організація їх анонімізації та псевдонімізації, забезпечення функціонування безпечних середовищ обробки, контроль

користувачів і держателів даних, ведення національного каталогу наборів даних та реєстру дозволів, забезпечення реалізації прав пацієнтів, встановлення вимог до якості даних, координація міжвідомчої взаємодії та забезпечення інтеграції України до транскордонної інфраструктури HealthData.

Вважаємо за доцільне визначити наступні повноваження Національного агентства з доступу до медичних даних (HDAB Ukraine) за групами:

1) регуляторно-дозвільна діяльність:

- розгляд заявок, видача, зміна, призупинення та анулювання дозволів на доступ;

- встановлення та розрахунок плати за надання доступу для покриття витрат на обробку, анонімізацію тощо;

- розробка методичних, регуляторних вимог, процедур доступу та вимог до безпечних середовищ обробки (SPE).

2) технічна обробка та кібербезпека:

- витребування та збір даних у держателів (ЕСОЗ, МІС, наукових установ);

- підготовка, об’єднання, структурування, псевдонімізація та анонімізація масивів даних;

- надання доступу виключно через безпечні середовища обробки (Secure Processing Environments).

- контроль вивантаження результатів з SPE для унеможливлення реідентифікації (вигрузка лише неперсональних/анонімізованих даних).

3) прозорість, якість та захист прав громадян:

- ведення Національного каталогу доступних наборів медичних даних;

- ведення Реєстру заявок, дозволів, відмов та публічних результатів;

- забезпечення прав пацієнтів, зокрема адміністрування механізму Opt-Out (права на відмову від вторинного використання);

- контроль вимог до якості, придатності та маркування даних у співпраці з їх держателями.

4) контроль, нагляд та санкції:

- контроль дотримання користувачами умов дозволу та цільового використання (для наукових досліджень, ШІ, статистики, інновацій);

- проведення перевірок та застосування коригувальних заходів/санкцій у разі порушень.

5) міжнародна співпраця та євроінтеграція:

- виконання функцій Національної контактної точки України для інфраструктури HealthData@EU;

- забезпечення безпечного транскордонного обміну даними з органами держав-членів ЄС;

- міжвідомча взаємодія з Органом із захисту персональних даних, МОЗ, НСЗУ, науковими установами та ринком ШІ.

Другий варіант - наділення відповідними повноваженнями існуючого суб'єкту може відбуватися за такими напрямами:

- наділення повноваженнями та формування структурного підрозділу на базі ДУ «Центр громадського здоров'я МОЗ України», який вже має досвід роботи з епідеміологічними даними, популяційними реєстрами, медичною статистикою та аналітикою для формування державної політики. Наказом ЦГЗ утворюється відокремлений Спеціалізований центр вторинного використання медичних даних із власною інфраструктурою для комплексної системи захисту інформації.

- наділення повноваженнями та формування структурного підрозділу в структурі Міністерства охорони здоров'я України. Це забезпечить максимальний рівень державного контролю, прямої регуляторної сили та швидкості прийняття нормативних рішень. Так, наказом МОЗ у структурі апарату утворюється новий самостійний підрозділ - Департамент з питань вторинного використання медичних даних (HDAB), який матиме обмежені

повноваження регуляторного, дозвільного, контрольного та наглядового характеру. Це зумовлено тим, що державні службовці не можуть проводити безпосередньо глибокі технічні процедури, а отже техніко-технологічні повноваження будуть покладатися на ДП «Електронне здоров'я».

- наділення повноваженнями та формування структурного підрозділу на базі ДП «Електронне здоров'я», яке вже є адміністратором Центральної бази даних ЕСОЗ (ЦБД ЕСОЗ) та володіє інфраструктурою для роботи з великими масивами даних. Реалізація можлива шляхом створення у структурі підприємства окремого Центру вторинного використання даних (HDAB Office) з розмежуванням прав доступу між адміністраторами ЦБД ЕСОЗ (первинні дані) та фахівцями HDAB (вторинні дані/SPE).

Залежно від сукупності політичних, економічних, соціальних можливостей України має бути обраний один з представлених варіантів.

2. Налагодження інформаційно-комунікаційної системи між цифровою системою національної системи охорони здоров'я з європейськими транскордонними мережами, що потрібно здійснити наступним чином:

- *організаційно-інституційне забезпечення* - надати функції та статус NCPH ДП «Електронне здоров'я», яке є адміністратором Центральної бази даних ЕСОЗ

- інформаційно-інфраструктурне забезпечення: побудова вузла взаємодії (NCPH Node); впровадження єдиного формату EEHRxF; гармонізація медичних кодифікаторів;

- нормативно-правове забезпечення: внесення змін до Постанови КМУ Про затвердження Порядку функціонування ЕСОЗ; розробка Порядку транскордонного обміну медичними даними; угода про приєднання до мережі MyHealth@EU.

3. Розширення інституційної спроможності для забезпечення використання штучного інтелекту в медицині. Реалізація зазначеного можлива наступними шляхами:

а) утворення спеціалізованого суб'єкту державного управління, що виступатиме Регулятором технологій штучного інтелекту - визначення національного компетентного органу, відповідального за координацію державної політики, нагляд за дотриманням вимог законодавства у сфері ШІ, координацію діяльності галузевих регуляторів, ведення реєстру високоризикових систем ШІ, моніторинг системних ризиків та взаємодію з відповідними інституціями Європейського Союзу. Варто зазначити, що серед країн-членів Європейського Союзу немає єдиного підходу, що представлено в таблиці 5.9.

Відповідно, для України пропонуємо утворити Національне агентство з регулювання технологій штучного інтелекту (зі спеціальним статусом). Даному Агентству доцільно передати горизонтальні функції, які стосуються всіх сфер застосування ШІ: координацію реалізації державної політики; контроль виконання рамкового Закону про ШІ; координацію галузевих регуляторів; формування та ведення реєстру високоризикових систем; методичне забезпечення оцінювання ризиків; координацію реагування на серйозні інциденти; міжнародну взаємодію та співпрацю з компетентними органами ЄС.

До повноважень Національного агентства з регулювання технологій штучного інтелекту пропонуємо віднести:

1) оцінка та нагляд:

- оцінка та категоризація ШІ-систем за рівнями ризику (неприйнятний, високий, обмежений, мінімальний);

- заборона використання ШІ-систем із неприйнятним рівнем ризику (наприклад, соціальний скоринг, маніпулятивні психологічні системи).

Таблиця 5.9

Інституційне забезпечення державного управління процесами впровадження технологій штучного інтелекту

Країна	Загальне регулювання	Галузеве регулювання	Нагляд	Характеристика
Фінляндія	Загальне виконання AI Act розподіляється між національними компетентними органами відповідно до сфер їх компетенції	Органи системи охорони здоров'я зберігають галузеві повноваження щодо безпечного використання цифрових технологій	Нагляд за медичними виробами та програмним забезпеченням медичного призначення здійснюється в межах сформованої системи регулювання медичних виробів	Децентралізована функціональна модель: нові вимоги AI Act інтегруються у сформовану систему галузевого регулювання, а не концентруються в одному «медичному регуляторі ШІ»
Данія	Реалізація AI Act ґрунтується на розподілі функцій між компетентними державними органами	Галузеві органи охорони здоров'я забезпечують регулювання цифрових технологій та їх використання в медичній практиці	ШІ, який має статус медичного виробу, підпадає одночасно під вимоги законодавства щодо медичних виробів та AI Act	Розподілена модель: загальне регулювання ШІ поєднується зі спеціальною компетенцією органів охорони здоров'я та медичних виробів
Франція	DGCCRF визначена центральною ланкою координації діяльності галузевих органів ринкового нагляду за AI Act та представництва відповідних французьких органів на рівні ЄС	Галузева компетенція залишається за спеціалізованими органами відповідної сфери	Ринковий нагляд за медичними виробами розподілений насамперед між ANSM і DGCCRF; ANSM має спеціальну компетенцію у сфері безпеки медичних виробів	Координаційно-децентралізована модель: центральний координатор + існуючі галузеві регулятори. Французький уряд прямо виходить із використання вже сформованої галузевої експертизи. (economie.gouv.fr)
Німеччина	Bundesnetzagentur виконує центральні функції у системі реалізації AI Act та забезпечує експертно-координаційну підтримку	Для сфер, які вже охоплені гармонізованим законодавством ЄС, передбачається збереження існуючих галузевих структур	Для медичних виробів як продукції Додатка I AI Act Німеччина орієнтується на використання існуючих структур ринкового нагляду, додавши до їх компетенції завдання за AI Act	Гібридна модель: центральна координація ШІ + децентралізований галузевий ринковий нагляд. Це один із найбільш релевантних прикладів для запропонованої української моделі. (Bundesnetzagentur)

Сформовано автором на основі: [219], [189], [190], [130], [157]

2) сертифікація та оцінка відповідності:

- ведення Реєстру ШІ-систем високого ризику;

- акредитація незалежних центрів тестування та оцінки відповідності алгоритмів;

- перевірка навчальних датасетів на відсутність дискримінаційних упереджень (bias);

- регуляторні пісочниці (Regulatory Sandboxes);

- створення безпечного правового та технічного середовища для випробування та тестування стартапами нових ШІ-технологій під наглядом держави до їх виходу на ринок.

3) розслідування та застосування санкцій:

- проведення аудитів алгоритмів/ШІ-систем у разі виникнення інцидентів (помилок, витоку даних, шкоди життю/здоров'ю);

- застосування адміністративно-господарських санкцій та штрафів за порушення вимог безпеки ШІ.

б) розширення повноважень ДЛЗ (Держлікслужби) щодо ринкового нагляду за ШІ-медичними виробами, пропонуємо здійснити наступним чином:

1) передринкова перевірка та оцінка відповідності:

- аудит документації: перевірка технічного файлу, системи управління ризиками (ISO 14971) та якості навчальних/валідаційних/тестових датасетів (перевірка на відсутність біасу/упередженості);

- валідація призначення: контроль відповідності заявленого медичного призначення реальним показникам точності, чутливості, специфічності та безпеки алгоритму.

2) постринковий нагляд та супровід оновлень:

- моніторинг оновлень: контроль за істотними змінами в коді та алгоритмах, що адаптуються/самонавчаються після введення в експлуатацію;

- реагування на інциденти: отримання, реєстрування та аналіз повідомлень про серйозні несприятливі події та збої ШІ;

- постринковий моніторинг: систематичний збір даних про реальну ефективність ШІ в клінічних умовах.

3) інспектування та допуск до даних:

- перевірка суб'єктів: проведення планових та позапланових інспекцій виробників, уповноважених представників, імпортерів та дистриб'юторів;

- доступ до логів та коду: витребування журналів роботи системи (logs), результатів тестування та, у разі обґрунтованої потреби, доступ до вихідного коду чи середовища розгортання.

4) застосування обмежувальних заходів та санкцій:

- коригувальні дії: винесення приписів щодо усунення невідповідностей у визначені терміни;

- обмеження обігу: тимчасове припинення або заборона застосування ШІ-медичного виробу;

- вилучення з ринку: рішення про вилучення або відкликання небезпечного чи фальсифікованого ШІ-продукту.

5) міжвідомча та міжнародна координація:

- внутрішня взаємодія: оперативний інформаційний обмін із МОЗ України, загальним Регулятором ШІ та HDAB Ukraine;

- міжнародна інтеграція: взаємодія з ЄС-базою даних EUDAMED та європейськими мережами ринкового нагляду.

3. Внесення змін до організаційної структури МОЗ щодо регулювання використання ШІ в медицині. Для уникнення створення нових надлишкових бюрократичних рівнів найбільш ефективним є поєднання створення профільного підрозділу (Департамент використання технологій штучного інтелекту в медицині) та розширення функцій існуючих директоратів

4. Розширення інституційної спроможності державного управління щодо захисту медичних даних пропонуємо здійснити шляхом створення незалежного наглядового органу - Національна комісія з питань захисту персональних даних та доступу до публічної інформації. Ключовими повноваженнями в реалізації механізмів державного управління цифровою трансформацією системи охорони здоров’я пропонуємо визначати наступні:

- регуляторний нагляд - 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»;

- затвердження стандартів та методологій - 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;

- аудит та контроль медичних ШІ-алгоритмів - перевірка прозорості та безпеки автоматизованих систем прийняття клінічних рішень і діагностичних нейромереж, щоб унеможливити алгоритмічні помилки, упередженість або несанкціоноване профілювання пацієнтів;

- реагування на інциденти та розслідування витоків - 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.

5. Розширення повноважень АМКУ пропонуємо здійснити шляхом внесення змін до Закону України «Про захист економічної конкуренції».

- право визначати «Цифрових гейткіперів»: встановити критерії для цифрових медичних платформ (за кількістю активних пацієнтів/лікарів на місяць та оборотом);

- заборона прямої та опосередкованої пріоритетизації: заборона гейткіперам застосовувати алгоритми, що надають вищий рейтинг власним послугам;

- забезпечення рівних умов: вимога застосовувати прозорі, об'єктивні та недискримінаційні параметри ранжування для всіх учасників ринку;

- право проводити аудит алгоритмів та аналізувати вихідний код: АМКУ має отримати доступ до технічної документації та алгоритмів видачі цифрових сервісів для перевірки на наявність прихованої пріоритетизації власних продуктів;

- застосування оборотних штрафів та строкових приписів: повноваження видавати приписи про негайну зміну алгоритму та накладати штрафи за порушення цієї заборони.

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 системи охорони здоров’я, який передбачає поєднання утворення нових спеціалізованих суб’єктів, розширення компетенцій існуючих органів та формування міжінституційної взаємодії. 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 економічної конкуренції.

Запропонований підхід ґрунтується на функціональному розподілі регуляторних, дозвільних, наглядових, контрольних, інформаційно-комунікаційних та координаційних повноважень відповідно до ключових об’єктів цифрової трансформації.

Запропонований механізм дозволяє сформувати інституційно цілісну систему державного управління цифровою трансформацією охорони здоров’я, 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. Його реалізація створює інституційні передумови для інтеграції цифрової системи охорони здоров’я 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 до 5-го розділу

1. Запропоновано комплексний механізм адаптації державного управління цифровою трансформацією системи охорони здоров'я до вимог Європейського Союзу, що визначає перехід від фрагментарної адаптації окремих актів до комплексної законодавчої архітектури цифрової охорони здоров'я. 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 наспрямовані на цифрових гейткіперів. 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 заміни 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.

2. 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. 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.

3. 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.

4. 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.

5. 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. 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. 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.

6. Реалізація запропонованого комплексного механізму створить передумови для керованого, безпечного та людиноцентричного впровадження штучного інтелекту в цифрову систему охорони здоров'я 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 Європейського Союзу. У ширшому контексті це дозволяє розглядати державне регулювання ШІ не як окремий напрям цифрової політики, а як складову державного управління цифровою трансформацією системи охорони здоров'я, від ефективності якої залежатимуть якість, доступність, безпека та інноваційність медичної допомоги.

7. 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 системи охорони здоров'я, який передбачає

поєднання утворення нових спеціалізованих суб'єктів, розширення компетенцій існуючих органів та формування міжінституційної взаємодії. 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 економічної конкуренції.

8. 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 охорони здоров'я, 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. Його реалізація створює інституційні передумови для інтеграції цифрової системи охорони здоров'я 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. Визначена сукупність факторів впливає 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. Цифрова трансформація системи охорони здоров'я 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-економічна 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 громадянського 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 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). 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 системи охорони здоров’я 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 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.

7. 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.

8. 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. Визначено, що створення Європейського простору даних охорони здоров’я 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 системи охорони здоров’я, 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 охорони здоров’я навіть в умовах воєнного стану. 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.

10. 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. 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 охорони здоров'я регуляторним актам Європейського Союзу та розроблено механізм її адаптації. Сформований підхід спрямований на подолання суттєвого розриву між наявною інфраструктурою електронної системи охорони здоров'я і європейськими директивами та регламентами. Для вирішення зазначеної проблеми запропоновано структуру та змістовне наповнення сукупності нових нормативно-правових актів, зокрема: Закон 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 штучного інтелекту в охороні здоров’я 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 системи охорони здоров’я України до європейського простору.

15. Проведене дослідження засвідчило необхідність розширення інституційної спроможності державного управління цифровою трансформацією системи охорони здоров’я, зумовлену появою нових об’єктів регулювання та необхідністю адаптації до вимог Європейського Союзу. 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 системи охорони здоров’я, 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 Європейського Союзу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналіз ведення електронних направлень лікарями первинної та спеціалізованої допомоги. URL: https://nszu.gov.ua/dashboards/analiz-vedennia-elektronnix-napravlen-likariami-per

2. Аналітичні панелі (дашборди). URL: https://nszu.gov.ua/nszu-cifrova/onlain-servisi-dasbordi

3. Бачук О.Р. Цифрова трансформація в системі охорони здоров'я. Вісник ОНУ імені І.І. Мечникова. 2024. Т. 29. Вип. 3 (101). С. 36-41.

4. Васюк Н.О. Трансформаційний механізм формування та реалізації державної політики у сфері охорони здоров’я: дис. на здобуття наук. ступеня д-ра наук з держ. упр. за спец. 25.00.02 Київський національний економічний університет імені Вадима Гетьмана. Київ, 2024. URL: https://kneu.edu.ua/ua/scientific_council/dd-26.006.010/defenddis/dd_250002/dd250002_/dd_24/

5. Висоцький А.А., Суріков О.О., Василюк-Зайцева С.В. Розвиток штучного інтелекту в сучасній медицині. Укр Мед Часопис. 2023. Вип. 2(154). С. 1-4. URL: https://umj.com.ua/wp/wp-content/uploads/2023/04/5262.pdf

6. Вовк А.В. Використання штучного інтелекту в медицині. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/47016/21267.pdf?sequence=3&isAllowed=y

7. Волков О.С. Штучний інтелект у медицині: перспективи діагностики та лікування до 2035 року. URL: https://repo.btu.kharkiv.ua/server/api/core/bitstreams/21b4c073-e662-4556-b246-c4b205763e4e/content

8. Воржакова Ю.П. Сутність цифрової трансформації з різних позицій підприємців та науковців. Економіка та держава. 2021. № 9. С. 107–111.

9. Гаєвська Л.А., Васюк Н.О., Гамкрелідзе К.Ю. Зарубіжний досвід реалізації державної політики цифрового розвитку: можливості для України.

Державне управління: удосконалення та розвиток. 2025. No 4. URL: https://www.nayka.com.ua/index.php/dy/article/view/6141

10. Горкуненко А.Б. Штучний інтелект у медицині: масштаби ринку та напрями розвитку. Вісник соціальної гігієни та організації охорони здоров’я України. 2025. Вип. 1. С. 35–41. DOI: https://doi.org/10.11603/1681-2786.2025.1.15340

11. Деякі питання електронної системи охорони здоров'я: Порядок від 25.04.2018 № 411. URL: https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text

12. Дія. Державні послуги онлайн. URL: https://diia.gov.ua/

13. Дія.City. URL: https://city.diia.gov.ua/

14. Електронна система охорони здоров'я в Україні. URL: https://ehealth.gov.ua/

15. Електронний рецепт на лікарські засоби: деталізація погашення. URL: https://nszu.gov.ua/dashboards/elektronnii-recept-na-likarski-zasobi-detalizaci

16. Електронний рецепт на лікарські засоби: деталізація створених рецептів. URL: https://nszu.gov.ua/dashboards/detalizaciia-vipisanix-elektronnix-receptiv-na-lik

17. Інформація про стан верифікації записів про пацієнтів, медичних працівників та суб’єктів господарювання (заклади охорони здоров’я, ФОП, аптечні заклади) в електронній системі охорони здоров’я. URL: https://nszu.gov.ua/dashboards/informaciia-pro-stan-verifikaciyi-zapisiv-pro-pacijen

18. Іртищева І.О., Сергійчук С.І., Рябець Д.М. Стан і перспективи цифрової трансформації індустрії охорони здоров'я в Україні. Збірник наукових праць ТДАТУ імені Дмитра Моторного (економічні науки). 2020. No1(41). С. 70-77. URL: https://Oj.Tsatu.Edu.Ua/Index.Php/Zbirnyk/Article/View/568/540

19. Кабінет Міністрів України / МОЗ України / ДП «Електронне здоров'я» Концепція розвитку електронної охорони здоров'я: Розпорядження Кабінету Міністрів України від 28.12.2020 р. № 1671-р. URL: https://zakon.rada.gov.ua/laws/show/1671-2020-%D1%80#Text

20. Колесніков А., Карапетян О. Штучний інтелект: переваги та загрози використання. Ефективна економіка. 2023. № 8. URL: https://www.nayka.com.ua/index.php/ee/article/view/1991

21. Криничко Л.Р. Теорія та методологія державного управління в сфері охорони здоров’я: монографія. Житомир : Вид. О.О. Євенок, 2020. 348 с.

22. Криничко Л.Р. Теорія та методологія державного управління в сфері охорони здоров’я: дис. на здобуття наук. ступеня д-ра наук з держ. упр. за спец. 25.00.02 – механізми державного управління. Державний університет «Житомирська політехніка». Житомир, 2021. URL: https://chmnu.edu.ua/wp-content/uploads/Disertatsiya.pdf

23. Куйбіда В.С., Карпенко О.В., Наместнік В.В. Цифрове врядування в Україні: базові дефініції понятійно-категоріального апарату. Вісник Національної академії державного управління при Президентові України. Серія : Державне управління. 2018. № 1. С. 5-10. URL: http://academy.gov.ua/infpol/pages/dop/2/files/974f8478$cfe8$4d31$971b$d5116efff458.pdf

24. Курбанов А.К. Державне управління потенціалом системи охорони здоров’я: дис. на здобуття наук. ступеня д-ра наук з держ. упр. за спеціальністю 25.00.02 – механізми державного управління. Державний університет «Житомирська політехніка», Житомир, 2026. URL: https://ztu.edu.ua/site/files/1/docs/dis_%D0%9A%D0%A3%D0%A0%D0%91%D0%90%D0%9D%D0%9E%D0%92NEW%20(1).pdf

25. Ліфінцев О.В. Поняття та особливості охорони здоров'я як об'єкта контролю. Науковий вісник Ужгородського національного університету. Серія «Право». 2014. Вип. 29, ч. 2, т. 3. С. 148–152. URL: http://www.irbis-

nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=nvuzhpr_2014_29(2.3)__37

26. Мандич О., Бабко Н., Лишенко М., Харчевнікова Л. Цифрова трансформація та новітні комунікації як платформа для стійкого розвитку бізнесу. Modeling the Development of the Economic Systems. 2022. № 4. С. 15–19.

27. Мартиненко О.В., Малярова Л.В. Цифрова трансформація охорони здоров'я: методичні рекомендації до практичних занять. Харків: ХНУ ім. В. Н. Каразіна, 2024. URL: https://ekhnuir.karazin.ua/server/api/core/bitstreams/d961507b-f54a-4ac7-a9ac-6f526af3b52c/content

28. Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua/

29. Міністерство цифрової трансформації України. Регулювання. URL: https://ai.thedigital.gov.ua/vision

30. Мойсеєнко М., Кузишин М., Туровська Л., Мазуренко Ю., Петришин М., Мазуренко О. Великі мовні моделі штучного інтелекту в медицині. Сучасні інформаційні технології та інноваційні методики навчання в підготовці фахівців: методологія, теорія, досвід, проблеми. 2024. Вип. 72. С. 73-88. URL: https://vspu.net/sit/index.php/sit/article/view/5637/5065

31. Музика-Стефанчук О.А., Стефанчук М.О., Якимчук Н.Я. Система охорони здоров’я в умовах цифровізації та реформування фінансування. Аналітично-порівняльне правознавство. 2023. № 5. С. 359-365. URL: https://app-journal.in.ua/wp-content/uploads/2023/11/66.pdf

32. Нікітін Ю.О., Кульчицький О.І. Цифрова парадигма як основа визначень: цифровий бізнес, цифрове підприємство, цифрова трансформація.

Маркетинг і цифрові технології. 2019. Т. 3. № 4. С. 77—87. URL: https://journals.indexcopernicus.com/api/file/viewBy$ FileId/907558.pdf

33. Омельченко С.О. Використання штучного інтелекту в медицині. URL: https://openarchive.nure.ua/server/api/core/bitstreams/29c96d0b-c089-4b92-9056-82825b34d754/content

34. Опанасюк М. Світові тенденції цифрової трансформації системи охорони здоров’я як об’єкта публічного управління. Економіка, управління та адміністрування. 2026. Вип. 1(115). С. 212–222. DOI: https://doi.org/10.26642/ema-2026-1(115)-212-222

35. Основи законодавства України про охорону здоров'я: Закон України від 19.11.1992 р. № 2801-XII, ст. 3 (чинна редакція). URL: https://zakon.rada.gov.ua/laws/show/2801-12#Text

36. Пазєєва Г. Принципи розбудови системи управління закладом охорони здоров’я. Вчені записки Університету «КРОК». 2025. Вип. 1(77). С. 273–280. URL: https://snku.krok.edu.ua/index.php/vcheni-zapiski-universitetu-krok/article/view/905/936

37. Пилипишин В.П. Поняття та основні риси державного управління Юридична наука і практика. 2011. № 2. С. 10-14. URL: https://essuir.sumdu.edu.ua/server/api/core/bitstreams/f487862a-47f3-4658-8ef1-5159c59de026/content

38. Про внесення змін до деяких законодавчих актів України щодо забезпечення укладення угоди між Україною та Європейським Союзом про взаємне визнання кваліфікованих електронних довірчих послуг та імплементації законодавства Європейського Союзу у сфері електронної ідентифікації: URL: https://zakon.rada.gov.ua/laws/show/2801-20#Text

39. Про внесення змін до статті 19 Закону України "Про лікарські засоби" щодо здійснення електронної роздрібної торгівлі лікарськими засобами: Закон України від 17.09.2020 № 904-IX. URL: https://zakon.rada.gov.ua/go/904-20

40. Про державний ринковий нагляд і контроль нехарчової продукції: Закон України від 02.12.2010 № 2735-VI. URL: https://zakon.rada.gov.ua/laws/show/2735-17#Text

41. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

42. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

43. Про електронну комерцію: Закон України від 03.09.2015 № 675-VIII. URL: https://zakon.rada.gov.ua/go/675-19

44. Про загальну безпечність нехарчової продукції: Закон України від 02.12.2010 № 2736-VI. URL: https://zakon.rada.gov.ua/laws/show/2736-17#Text

45. Про затвердження Технічного регламенту щодо медичних виробів від 02.10.2013 № 753. URL: https://zakon.rada.gov.ua/laws/show/753-2013-%D0%BF#Text

46. Про затвердження Технічного регламенту щодо медичних виробів для діагностики in vitro від 02.10.2013 № 754. URL: https://zakon.rada.gov.ua/laws/show/754-2013-%D0%BF#Text

47. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

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

49. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

50. Про медіа: Закон України від 13.12.2022 № 2849-IX. URL: https://zakon.rada.gov.ua/laws/show/2849-20

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

52. Про публічні електронні реєстри: Закон України від 18.11.2021 № 1907-IX. URL: https://zakon.rada.gov.ua/laws/show/1907-20#Text

53. Про ратифікацію Угоди між Україною та Європейським Союзом про участь України у програмі Європейського Союзу "Цифрова Європа" (2021-2027) від 23.02.2023 р. URL: https://zakon.rada.gov.ua/laws/show/2926-20#Text

54. Про стимулювання розвитку цифрової економіки в Україні. Закон України від 15.07.2021 № 1667-IX. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text

55. Про схвалення Концепції розвитку штучного інтелекту в Україні від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

56. Про схвалення Стратегії розбудови телемедицини в Україні: План від 14.07.2023 № 625-р. URL: https://zakon.rada.gov.ua/laws/show/625-2023-%D1%80#Text

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

58. Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 р. № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text

59. Проект Закону про Національну комісію з питань захисту персональних даних та доступу до публічної інформації № 6177 від 18.10.2021 р. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72992

60. Проєкт Постанови про прийняття за основу проекту Закону України про внесення зміни до статті 24 Закону України “Про Службу безпеки України”. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40689

61. Проневич О.М. Охорона здоров'я населення як сфера адаптації законодавства України до актів acquis communautaire. Вісник ХНУВС. 2017. № 2 (77). С. 155–164. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=VKhnuvs_2017_2_21

62. Регулювання штучного інтелекту в Україні: презентуємо дорожню карту. 2023. URL: https://thedigital.gov.ua/news/technologies/regulyuvannya-shtuchnogo-intelektu-v-ukraini-prezentuemo-dorozhnyu-kartu

63. Руденко Р.І. Цифрова трансформація охорони здоров’я України в 2025 році: вплив на якість життя. Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування. 2026. Том 37 (76) № 1. С. 150-155. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2026/1_2026/23.pdf

64. Рябець Д.М. Державне регулювання сфери охорони здоров’я: принципи, механізм та інструменти. Економічні горизонти. 2018. No4(7). С.164–174. URL: https://eh.udpu.edu.ua/article/view/212757/212805

65. Сільченко В. Підходи до трактування дефініції «цифрова трансформація». Економіка та суспільство. 2024. Вип. 66. URL: https://doi.org/10.32782/2524-0072/2024-66-132

66. Соболєв В. М., Хорошев М. І. Особливості та перспективи цифрової модернізації соціального захисту в Україні. Бізнес Інформ. 2025. №11. С. 205–216. URL: https://www.business-inform.net/export_pdf/business-inform-2025-11_0-pages-205_216.pdf

67. Статистика ведення електронних медичних записів в ЕСОЗ. URL: https://nszu.gov.ua/dashboards/statistika-vedennia-elektronnix-medicnix-zapisiv-v

68. Статистика поданих декларацій про вибір лікаря первинної медичної допомоги. URL: https://nszu.gov.ua/dashboards/statistika-podanix-deklaracii-pro-vibir-likaria-per

69. Струтинська І.В. Дефініції поняття "цифрова трансформація". Науково-практичний журнал "Причорноморські економічні студії". 2019. Вип. 48(2). С. 91-96. URL: http://bses.in.ua/journals/2019/ 48_2_2019/19.pdf

70. Сучасні досягнення ШІ для радіологічної діагностики. URL: https://radiolance.ua/suchasni-dosiagnennia-shi-dlia-radiologichnoyi-diagnostyky/

71. Терзі О.О. Визначення поняття «охорона здоров'я». Науковий вісник Ужгородського національного університету. Серія «Право». 2018. Вип. 51, т. 2. С. 46–49. URL: https://repo.odmu.edu.ua/xmlui/bitstream/handle/123456789/7030/Terzi.pdf?sequence=1&isAllowed=y

72. Україна серед лідерів GovTech у рейтингу Світового банку. Міністерство цифрової трансформації України. URL: https://thedigit.banku.

73. Центральний засвідчувальний орган. Міністерство цифрової трансформації України. URL: https://czo.gov.ua/

74. Цифрова трансформація охорони здоров’я: підсумки 2025 року. URL: https://ehealth.gov.ua/2025/12/30/tsyfrova-transformatsiya-ohorony-zdorov-ya-pidsumky-2025-roku/

75. Шамич О.М. Поняття та структура природного права людини на охорону здоров'я. Актуальні проблеми навчання та виховання людей з особливими потребами. 2014. № 11 (13). С. 75-92.

76. Швець Ю. Зміст конституційного права особи на охорону здоров'я. Підприємництво, господарство і право. 2017. № 8. С. 135–138. URL: https://pgp-journal.kiev.ua/archive/2017/8/29.pdf

77. Шлапко Т.В., Старинський М.В., Миргород-Карпова В.В., Висоцький А.І., Шеін Д.С. Правове забезпечення трансформації сфери охорони здоров’я у світлі медичної реформи з огляду на євроінтеграційні процеси. Аналітично-порівняльне правознавство. 2021. № 3. С. 141-147. URL: https://essuir.sumdu.edu.ua/server/api/core/bitstreams/d6562b85-9a97-4580-b70a-a900647cee19/content

78. Юнгер В.І. Стратегічні положення державного управління процесами повоєнного відновлення системи охорони здоров'я: дис. на здобуття наук. ступеня д-ра наук з держ. упр. за спец. 25.00.02 – механізми державного управління. Державний університет «Житомирська політехніка». Житомир, 2024.

79. Яценко В.А., Попов С.А., Воронов О.І. Публічна політика в умовах цифрових трансформацій: управління конфліктами та комунікаціями в системі охорони здоров'я. Успіхи і досягнення у науці. 2025. № 4(14). С. 905-917. URL: https://perspectives.pp.ua/index.php/sas/article/view/22968

80. #SmartHealthSystems. Startseite. URL: https://www.bertelsmann-stiftung.de/en/our-projects/the-digital-patient/projektthemen/smarthealthsystems

81. 2025 digital decade ehealth indicator study - Publications Office of the EU. Publications Office of the EU. URL: https://op.europa.eu/en/publication-detail/-/publication/bb5838fe-4742-11f0-85ba-01aa75ed71a1/language-en.

82. A Critical Analysis of the EU Data Act Proposal To what extend does the EU Data Act's Interplay with the General Data Protection Regulation impact its objective of facilitating access to data? URL: https://drepo.sdl.edu.sa/items/894f351f-4c3a-46e1-8383-ad6aaccbc5e0?utm_source=chatgpt.com

83. Abellán Álvarez I., Hölzmer P., Sedlmeir J. Privacy evaluation of the European Digital Identity Wallet's Architecture and Reference Framework. Computers & Security. 2026. Vol. 160, 104707. URL: https://www.sciencedirect.com/science/article/pii/S0167404825003967?utm_source=chatgpt.com#section-cited-by

84. Ability to facilitate health technologies in Europe 2022. Statista. Statista. URL: https://www.statista.com/statistics/1421889/ability-to-facilitate-health-technologies-in-europe/.

85. Adler-Milstein J., Jha A. K. HITECH Act Drove Large Gains In Hospital Electronic Health Record Adoption. Health Affairs. 2017. № 36(8). P. 1416–1422.

86. Agarwal R., Gao G., DesRoches C., Jha A.K. Research Commentary – The Digital Transformation of Healthcare: Current Status and the Road Ahead. Information Systems Research. 2010. Vol. 21, No. 4. P. 796–809.

87. Agbo C.C., Mahmoud Q.H., Eklund J.M. Blockchain technology in healthcare: A systematic review. Healthcare. 2019. № 7(2). P. 56.

88. Akman P. Regulating competition in digital platform markets: a critical assessment of the framework and approach of the EU Digital Markets Act. European Law Review, 2022. Vol. 47 (1). pp. 85-114.

89. Albisinni S., Rassweiler J., van Poppel H. The Future of Medical Devices in Europe Is at Stake: Concerns over the Implementation of the Medical Devices Regulation 2017/745. Eur Urol. 2023. Vol. 83(3). Pp. 191-192. doi: 10.1016/j.eururo.2022.12.015. Epub 2023 Jan 4. PMID: 36609009.

90. Almyranti, M. et al. Artificial Intelligence and the health workforce: Perspectives from medical associations on AI in health. OECD Artificial Intelligence Papers. 2024. No. 28, OECD Publishing, Paris, https://doi.org/10.1787/9a31d8af-en.

91. Andmehalduse mõisted. URL: https://www.stat.ee/et/statistikaamet/andmehaldus/andmehalduse-moisted?utm_source=chatgpt.com

92. Applications of AI in healthcare Europe 2024. Statista. URL: https://www.statista.com/statistics/1558711/applications-of-ai-in-healthcare-europe/

93. Arrêté royal exécutant la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique. URL: https://www.ejustice.just.fgov.be/eli/arrete/2024/06/09/2024005260/moniteur

94. Arrêté royal portant exécution de la loi du 15 juin 2022 relative aux dispositifs médicaux de diagnostic in vitro. URL: https://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=23-01-10&numac=2023030047&utm_source=chatgpt.com

95. Arrêté royal relatif aux études des performances de dispositifs médicaux de diagnostic in vitro. URL: https://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=22-10-25&numac=2022042240&utm_source=chatgpt.com

96. Arrêté royal relatif aux investigations cliniques de dispositifs médicaux. URL: https://www.fagg.be/sites/default/files/KB_18052021.pdf?utm_source=chatgpt.com

97. Arroyo J., Vu H., Yu-Cheong Yeung T. The European Health Data Space: Will it be emergency-ready? URL: https://www.sciencedirect.com/science/article/abs/pii/S221188372500005X?utm_source=chatgpt.com

98. Artificial Intelligence (AI) in Healthcare Market Size, Share & Industry Analysis, By Platform (Solutions and Services), By Application (Robot-Assisted Surgery, Virtual Nursing Assistant, Administrative Workflow Assistance, Clinical Trials, Diagnostics, and Others), By End-user (Hospitals & Clinics, Pharmaceutical & Biotechnology Companies, Contract Research Organization (CRO), and Others), and Regional Forecasts, 2026-2034. URL: https://www.fortunebusinessinsights.com/industry-reports/artificial-intelligence-in-healthcare-market-100534

99. Artificial intelligence in healthcare. Applications, risks, and ethical and societal impacts. URL: https://op.europa.eu/en/publication-detail/-/publication/958117aa-0c91-11ed-b11c-01aa75ed71a1/language-en?utm_source=chatgpt.com

100. Ashley E.A. The precision medicine initiative: A new national effort. JAMA. 2016. № 315(8). P. 795–796.

101. Atzori M. The Digital Services Act and the Freedom of Expression in the European Union: A Political Perspective (June 21, 2024). URL: SSRN: https://ssrn.com/abstract=4887181 or http://dx.doi.org/10.2139/ssrn.4887181

102. Bajwa J., Munir U., Nori A., Williams B. Artificial intelligence in healthcare: transforming the practice of medicine. Future Healthc J 2021 Jul. Vol. 8(2):e188–e194. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC8285156/

103. Bekendtgørelse af lov om medicinsk udstyr (LBK nr. 682 af 29/05/2023). København: Indenrigs- og Sundhedsministeriet, 2023. URL: https://www.retsinformation.dk/eli/lta/2023/682?utm_source=chatgpt.com

104. Bekendtgørelse af sundhedsloven (LBK nr. 275 af 12. marts 2025). København, 2025. URL: https://www.retsinformation.dk/eli/lta/2025/275?utm_source=chatgpt.com

105. Bekendtgørelse nr. 255 af 24. februar 2022 om drift m.v. af den fælles digitale infrastruktur. København, 2022. URL: https://www.retsinformation.dk/eli/lta/2022/255?utm_source=chatgpt.com

106. Belgian Health Data Agency. URL: https://www.hda.belgium.be/en?utm_source=chatgpt.com

107. Bescherming van medische gegevens. URL: https://www.rijksoverheid.nl/themas/familie-zorg-en-gezondheid/digitale-gegevens-in-de-zorg/bescherming-van-medische-gegevens?utm_source=chatgpt.com

108. Bhatt A.S., Varshney A.S., Moscone A., et al. Virtual care team guided management of patients with heart failure during hospitalization. J Am Coll Cardiol. 2023. Vol. 81(17). pp. 1680-1693. URL: https://www.jacc.org/doi/10.1016/j.jacc.2023.02.029

109. Biancone P., Secinaro S., Marseglia R., Calandra D. E-health for the future. Managerial perspectives using a multiple case study approach. Technovation. 2023. № 120. URL:

110. Boosting digital health can help prevent millions of deaths from noncommunicable diseases. World Health Organization (WHO). URL: https://www.who.int/news/item/23-09-2024-boosting-digital-health-can-help-prevent-millions-of-deaths-from-noncommunicable-diseases?utm.

111. Bou'e C., Schaible S. Die Digitale Transformation der Industrie. Roland Berger Strategy Consultans und Bundesverband der Deutschen Industrie, Munchen, Berlin, Germany. 2015.

112. Bundesinstitut für Arzneimittel und Medizinprodukte. URL: https://diga.bfarm.de/de

113. Buntin M.B., Burke M.F., Hoaglin M.C., Blumenthal D. The benefits of health information technology: A review of the recent literature shows predominantly positive results. Health Affairs. 2011. № 30(3). P. 464–471.

114. Cabitza F., Rasoini R., Gensini G.F.. Unintended consequences of machine learning in medicine. JAMA. 2017. Vol. 318(6). pp. 517-518. URL: https://pubmed.ncbi.nlm.nih.gov/28727867/

115. Carovano G., Finck M. Regulating data intermediaries: The impact of the Data Governance Act on the EU’s data economy, Computer Law & Security Review. 2023. Vol. 50, 105830. URL: https://www.sciencedirect.com/science/article/pii/S0267364923000407?utm_source=chatgpt.com

116. Caton J., Juillet Y. Rapport 23-15. Rapport inter-académique. La mise en application du règlement européen 2017/745/EU sur les dispositifs médicaux. Bulletin de l'Académie Nationale de Médecine. 2023. Vol. 207, I. 8.pp. 1007-1013. URL:

https://www.sciencedirect.com/science/article/pii/S0001407923002017?utm_source=chatgpt.com

117. Centre for Cybersecurity Belgium. NIS 2. URL: https://ccb.belgium.be/regulation/nis2

118. Centre for Cybersecurity Belgium. URL: https://ccb.belgium.be/?utm_source=chatgpt.com

119. Char D.S., Shah N.H., Magnus D. Implementing machine learning in health care – addressing ethical challenges. New England Journal of Medicine. 2018. № 378(11). P. 981–983.

120. Chen I.Y., Pierson E., Rose S., Joshi S., Ferryman K., Ghassemi M. Ethical machine learning in healthcare. Annu Rev Biomed Data Sci. 2021. Vol. 4. Pp. 123-144. URL: https://www.annualreviews.org/content/journals/10.1146/annurev-biodatasci-092820-114757

121. Cole A., Towse A. OP279 Data Protection In The European Union Post-General Data Protection Regulation (GDPR): A Barrier Or An Enabler Of Pharmaceutical Innovation? International Journal of Technology Assessment in Health Care. 2021;37(S1):10-11. doi:10.1017/S0266462321000908

122. Cresswell K.M., Worth A., Sheikh A. Implementing and adopting electronic health record systems: How actor-network theory can support evaluation. Clinical Governance: An International Journal. 2013. № 18(2). P. 106–113.

123. Cybersecurity Act. URL: https://www.riigiteataja.ee/en/akt/526082022002?leiaKehtiv

124. Dal Mas F., Massaro M., Rippa P., Secundo G. The challenges of digital transformation in healthcare: An interdisciplinary literature review, framework, and future research agenda. Technovation. 2023. № 123. DOI: 10.1016/j.technovation.2023.102716

125. Danish Agency for Digital Government. URL: https://digst.dk/?utm_source=chatgpt.com

126. Danish Health Data Authority. URL: https://sundhedsdatastyrelsen.dk/cybersikkerhed/?utm_source=chatgpt.com

127. Danish Regions. URL: https://www.regioner.dk/?utm_source=chatgpt.com

128. Databeskyttelsesloven (LBK nr. 289 af 08/03/2024). Bekendtgørelse af lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger. København, 2024.

129. Davenport T., Kalakota. R. The potential for artificial intelligence in healthcare. Future Healthc J. 2019. Vol. 6(2). pp. 94-98. URL: https://pubmed.ncbi.nlm.nih.gov/31363513/

130. Die Marktüberwachung spielt eine zentrale Rolle bei der Gewährleistung der Sicherheit, Zuverlässigkeit und des fairen Wettbewerbs. URL: https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/14_Marktueberwachung/start.html?utm_source=chatgpt.com

131. Digital Health Market (2026 - 2033). Size, Share & Trends Analysis Report By Technology (Healthcare Analytics, mHealth), By Component (Hardware, Software, Services), By Application, By End Use, By Region, And Segment Forecasts. URL: https://www.grandviewresearch.com/industry-analysis/digital-health-market

132. Digital Health Market Trends, Healthcare Spending, Technology Adoption, Reimbursement Analysis, Cost Structure, Market Penetration, and Growth Outlook. URL: https://www.precedenceresearch.com/digital-health-market

133. Digital health: The power behind power. URL: https://www.efpia.eu/about-medicines/use-of-medicines/healthcare-systems/digital-

health/#:~:text=The%20overarching%20principles%20should%20be%20people%2Dcentricity%20and,purposes%20for%20which%20their%20data%20are%20used%3B

134. Digital Sundhed Danmark. URL: https://sundhedsdatastyrelsen.dk/om-os/organisation/digital-sundhed-danmark?utm_source=chatgpt.com

135. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1688480129686&uri=CELEX%3A32022L2555&utm_source=chatgpt.com

136. Dombrink I., Lubbers B.R., Simulescu L., Doeswijk R., Tkachenko O., Dequeker E., Fraser A.G., van Dongen J.J.M., Cobbaert C., Brüggemann M., Macintyre E. Critical Implications of IVDR for Innovation in Diagnostics: Input From the BioMed Alliance Diagnostics Task Force. Hemasphere. 2022. Vol. 6(6):e724. doi: 10.1097/HS9.0000000000000724. PMID: 35620593; PMCID: PMC9126521.

137. Dorsey E.R., Topol E.J. State of telehealth. New England Journal of Medicine. 2016. № 375(2). P.154–161.

138. Dove E S. The European Health Data Space as a Case Study, Ethics & Human Research. 2024. Vol. 46, no. 6 (2024), pp. 29–35. DOI: 10.1002/eahr.500228

139. Duivenvoorde B., Goanta C. The regulation of digital advertising under the DSA: A critical assessment. URL: https://research-portal.uu.nl/en/publications/the-regulation-of-digital-advertising-under-the-dsa-a-critical-as/?utm_source=chatgpt.com

140. Ebers M. Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act. European Journal of Risk Regulation. 2025, Vol. 16(2). pp. 684-703. doi:10.1017/err.2024.78

141. eHealth Belgium. URL: https://www.ehealth.fgov.be/nl

142. Electronic Communications Act. URL: https://www.riigiteataja.ee/en/akt/501042015003?leiaKehtiv

143. Electronic cross-border health services. Public Health. URL: https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/electronic-cross-border-health-services_en.

144. Electronic Health Records Market Size, Share, Growth, and Regional Forecast, 2026 to 2033. URL: https://www.persistencemarketresearch.com/market-research/electronic-health-records-market.asp

145. Electronic Identification and Trust Services for Electronic Transactions Act. Passed 12.10.2016. URL: https://www.riigiteataja.ee/en/akt/527102016001

146. Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (1) (C/2024/2836). URL: https://eur-lex.europa.eu/eli/C/2024/2836/oj/eng/pdf?utm_source=chatgpt.com

147. Esteves B., Rodríguez Doncel V., Pandit H.J., Lewis D. Semantics for implementing data reuse and altruism under eu's data governance act. In: Knowledge Graphs: Semantics, Machine Learning, and Languages: Proceedings of the 19th International Conference on Semantic Systems, 20–22 September 2023, Leipzig, Germany. SAGE

148. Estonian Data Protection Inspectorate. URL: https://www.aki.ee/en?utm_source=chatgpt.com

149. Ethics and governance of artificial intelligence for health. World Health Organization (WHO). URL: https://www.who.int/publications/i/item/9789240029200?utm.

150. Ethics guidelines for trustworthy AI. 2019. URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai?ref=curiocial.com

151. EU MDR Checklist: Technical Documentation Requirements for Medical Device Manufacturers. URL: https://www.celegence.com/eu-mdr-checklist-technical-documentation-requirements-for-medical-device-manufacturers/#:~:text=This%20guide%20outlines%20the%20key%20technical%20documentation,2017%2F745)%20extends%20well%20beyond%20obtaining%20CE%20marking.

152. European Health Data Space must ensure strong protection for electronic health data. URL: https://www.edps.europa.eu/press-publications/press-news/press-releases/2022/european-health-data-space-must-ensure-strong_de?utm_source=chatgpt.com

153. European Health Data Space Regulation (EHDS). URL: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en?utm_source=chatgpt.com

154. Federal agency for medicines and health products. URL: https://www.famhp.be/en

155. Ferguson D.D.S. The outcome efficacy of the entity risk management requirements of the NIS 2 Directive. International Cybersecurity Law Review. 2023. Vol. 4. pp. 371–386. URL: https://link.springer.com/article/10.1365/s43439-023-00097-8?utm_source=chatgpt.com

156. Fernandez-Marcelo P.G., Bernabe P.M.B., Bonito S.R., Medina P.B.A framework for the development of interoperability standards for electronic health records: A systematic review. Studies in Health Technology and Informatics. 2016. № 225. P. 232–236.

157. Forslag til lov om ændring af sundhedsloven og forskellige andre love. Folketinget. URL: https://www.retsinformation.dk/eli/ft/202413L00154?utm_source=chatgpt.com

158. Free C., Phillips G., Watson L., Galli L., Felix L., Edwards P., Patel V., Haines A. The effectiveness of mobile-health technology-based health behaviour change or disease management interventions for health care consumers: A systematic review. PLOS Medicine. 2013. № 10(1). DOI: 10.1371/journal.pmed.1001362

159. Garsia S., Bilgesu S. The european digital identity wallet as a tool to increase individual autonomy: from theory to critical reality (March 24, 2026). URL: https://ssrn.com/abstract=6462902 DOI: http://dx.doi.org/10.2139/ssrn.6462902

160. Gerke S., Minssen T., Cohen I.G. Ethical and legal challenges of artificial intelligence-driven healthcare. In: Bohr A, Memarzadeh K, eds. Artificial Intelligence in Healthcare. Academic Press; 2020. pp. 295-336. URL: https://www.sciencedirect.com/science/chapter/edited-volume/pii/B9780128184387000125

161. Ghasemzadeh Kh., Escobar O. etc. User innovation rings the bell for new horizons in e-health: a bibliometric analysis. European Journal of Innovation Management. 2022. URL: https://www.emerald.com/insight/content/doi/10.1108/EJIM-04-2021-0181/full/html

162. Global Digital Health Monitor. datadot. URL: http://data.who.int/dashboards/gdhm/overview?year=2024.

163. Global Digital Health Monitor. URL: https://monitor.digitalhealthmonitor.org/regional_overview/EMRO

164. Global Observatory for eHealth. URL: https://www.who.int/observatories/global-observatory-for-ehealth

165. Global strategy on digital health 2020-2027. World Health Organization (WHO). URL: https://www.who.int/publications/i/item/9789240116870?utm.

166. Gong C., Ribiere V. Developing a unified definition of digital transformation. Technovation. 2021. № 102. URL: https://ideas.repec.org/a/eee/techno/v102y2021ics0166497220300894.html

167. Gopal G., Suter-Crazzolara C., Toldo L., Eberhardt W. Digital transformation in healthcare – architectures of present and future information technologies. Clinical Chemistry and Laboratory Medicine. 2019. Vol. 57, No. 3. P. 328–335.

168. Government Office of Estonia. EestiAI initiative. URL: https://www.riigikantselei.ee/en/supporting-government-and-prime-minister/eestiai-initiative?utm_source=chatgpt.com

169. Health and Welfare Information Systems Centre (TEHIK). URL: https://www.tehik.ee/en/foreign-delegations

170. Health Belgium. URL: https://www.health.belgium.be

171. Health Board of Estonia. URL: https://www.terviseamet.ee/en?utm_source=chatgpt.com

172. Health information system. URL: https://www.tehik.ee/en/health-information-system?utm_source=chatgpt.com

173. Health Services Organisation Act. URL: https://www.riigiteataja.ee/en/akt/520052026006

174. Hesse B. W. Riding the Wave of Digital Transformation in Behavioral Medicine. Annals of behavioral medicine : a publication of the Society of Behavioral Medicine. 2020. № 54(12). P. 960–967. DOI: https://doi.org/10.1093/abm/kaaa093

175. Hsiao C.J., Hing E., Ashman J. Trends in Electronic Health Record System Use Among Office-based Physicians: United States, 2007-2012. National Health Statistics Reports. 2014. № 75. P. 1–18.

176. Hussain S.A., Bresnahan M., Zhuang J. The bias algorithm: how AI in healthcare exacerbates ethnic and racial disparities—a scoping review. Ethnicity &

Health. 2025. Vol. 30(2). pp. 197–214. URL: https://www.tandfonline.com/doi/citedby/10.1080/13557858.2024.2422848?scroll=top&needAccess=true

177. Information Security Committee. URL: https://www.inprosec.com/en/what-is-an-it-security-committee/

178. Information security in 2020 Annual report of the National Cyber Security Centre Finland. URL: 2021. URL: https://www.kyberturvallisuuskeskus.fi/files/media/publication/TRAFICOM_Tietoturvan-vuosi-2020_EN_210608_WEB%20(1).pdf

179. Information System Authority. CERT-EE. URL:https://www.ria.ee/en/cyber-security/cert-ee?utm_source=chatgpt.com

180. Institut national d'assurance maladie-invalidité. URL: https://www.inami.fgov.be/fr

181. Institute of Genomics. URL: https://genomics.ut.ee/en

182. Isikut tõendavad dokumendid ja identiteedihaldus. URL: https://www.siseministeerium.ee/ru/deyatelnost/effektivnoe-upravlenie-narodonaseleniem/udostoveryayuschie-lichnost-dokumenty-i

183. Islam S.M.R., Kwak D., Kabir M.H., Hossain M., Kwak K.S. The Internet of Things for health care: A comprehensive survey. IEEE Access. 2015. № 3. P. 678–708.

184. Karagianni A. Gender in a stereo-(gender)typical EU AI law: A feminist reading of the AI act. Cambridge Forum on AI: Law and Governance. 2025;1:e25. doi:10.1017/cfl.2025.12

185. Kelly C.J., Karthikesalingam A., Suleyman M., Corrado G., King D. Key challenges for delivering clinical impact with artificial intelligence. BMC Med. 2019. Vol. 17(1). Pp. 195.URL: https://pubmed.ncbi.nlm.nih.gov/31665002/

186. Kjørven M.E., Gjøsteen K., Wærstad T.L. Safe and inclusive or unsafe and discriminatory? European digital identity wallets and the challenges of “sole

control”. Computer Law & Security Review. 2026. Vol. 60, 106235. URL: https://www.sciencedirect.com/science/article/pii/S2212473X25001075

187. Koninklijk besluit tot wijziging en opheffing van diverse bepalingen met betrekking tot medische hulpmiddelen. URL: https://www.ejustice.just.fgov.be/eli/besluit/2021/04/28/2021041342/justel

188. Kujbida V.S., Karpenko O.V., Namestnik V.V. Digital governance in Ukraine: basic definitions of the conceptual$categorical apparatus, Visnyk NADU pry Prezydentovi Ukrainy (Seriia "Derzhavne upravlinnia"). 2018. vol. 1, pp. 5-10. URL: http://academy.$ gov.ua/infpol/pages/dop/2/files/974f8478$cfe8$4d31$971b$d5116efff458.pdf

189. Laki lääkinnällisistä laitteista. 719/2021. URL: https://www.finlex.fi/fi/lainsaadanto/2021/719?utm_source=chatgpt.com

190. Les autorités compétentes pour la mise en œuvre du règlement européen sur l’intelligence artificielle. URL: https://www.entreprises.gouv.fr/priorites-et-actions/transition-numerique/soutenir-le-developpement-de-lia-au-service-de-0?utm_source=chatgpt.com

191. Local Government Denmark. URL: https://www.kl.dk/?utm_source=chatgpt.com

192. Loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth. URL: https://www.ehealth.fgov.be/ehealthplatform/fr/loi-du-21-aout-2008-relative-a-l-institution-et-a-l-organisation-de-la-plate-forme-ehealth?utm_source=chatgpt.com

193. Loi établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (1). URL: https://www.ejustice.just.fgov.be/cgi/article.pl?language=fr&sum_date=2024-05-17&lg_txt=f&caller=sum&s_editie=1&2024202344=4&numac_search=2024202344&view_numac=2024202344f

194. Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel(NOTE : Consultation des versions

antérieures à partir du 05-09-2018 et mise à jour au 08-07-2024). URL: https://www.ejustice.just.fgov.be/eli/loi/2018/07/30/2018040581/justel?utm_source=chatgpt.com#LNK0003

195. Loi relative aux dispositifs médicaux de diagnostic in vitro (1). URL: https://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=22-06-30&numac=2022032523&utm_source=chatgpt.com

196. Loi relative aux dispositifs médicaux. URL: https://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=21-01-18&numac=2021030071&utm_source=chatgpt.com

197. Lov nr. 1533 af 12. december 2023 om supplerende bestemmelser til Europa-Parlamentets og Rådets forordning om digitale markeder. København, 2023. URL: https://www.retsinformation.dk/eli/lta/2023/1533?utm_source=chatgpt.com

198. Lov nr. 1618 af 16. december 2025 om supplerende bestemmelser til forordningen om harmoniserede regler om fair adgang til og anvendelse af data (datadelingsloven). København, 2025. URL: https://www.retsinformation.dk/eli/lta/2025/1618?utm_source=chatgpt.com

199. Lov nr. 1758 af 29. december 2025 om Digital Sundhed Danmark. København, 2025. URL: https://www.retsinformation.dk/eli/lta/2025/1758?utm_source=chatgpt.com

200. Lov nr. 1760 af 29. december 2025 om ændring af sundhedsloven og forskellige andre love (National planlægningskompetence for digitalisering og data i sundhedsvæsenet, nye regler for fælles digital infrastruktur, ændringer som følge af lov om Digital Sundhed Danmark m.v.). København, 2025. URL: https://www.retsinformation.dk/eli/lta/2025/1760?utm_source=chatgpt.com

201. Lov nr. 1765 af 28. december 2023 om håndhævelse af Europa-Parlamentets og Rådets forordning om et indre marked for digitale tjenester. København, 2023. URL: https://www.retsinformation.dk/eli/lta/2023/1765?utm_source=chatgpt.com

202. Lov nr. 42 af 21. januar 2025 om supplerende bestemmelser til Europa-Parlamentets og Rådets forordning (EU) 2022/868 af 30. maj 2022 om europæisk datastyring og om ændring af forordning (EU) 2018/1724 (datastyringsloven). København, 2025. URL: https://www.retsinformation.dk/eli/lta/2025/42?utm_source=chatgpt.com

203. Lov nr. 467 af 14. maj 2025 om supplerende bestemmelser til forordningen om kunstig intelligens. København, 2025. URL: https://www.retsinformation.dk/eli/lta/2025/467?utm_source=chatgpt.com

204. Lov nr. 617 af 8. juni 2016 om supplerende bestemmelser til forordning om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked. København, 2016. URL: https://www.retsinformation.dk/eli/lta/2016/617?utm_source=chatgpt.com

205. Lov nr. 780 af 4. maj 2021 om supplerende bestemmelser til forordningen om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (lov om cybersikkerhedscertificering). København, 2021. https://www.retsinformation.dk/eli/lta/2021/780?utm_source=chatgpt.com

206. Lovgivning om sikkerhed og beredskab i telesektoren. URL: https://samsik.dk/tele/lovgivning-sikkerhed-beredskab-telesektoren/

207. Marelli L., Stevens M., Sharon T., Van Hoyweghen I., Boeckhout M., Colussi I., Degelsegger-Márquez A., El-Sayed S., Hoeyer K., van Kessel R., Zając D.K., Matei M., Roda S., Prainsack B., Schlünder I., Shabani M., Southerington T. The European health data space: Too big to succeed? Health Policy. 2023 Sep;135:104861. doi: 10.1016/j.healthpol.2023.104861. Epub 2023 Jun 26. PMID: 37399677; PMCID: PMC10448378.

208. Marques I.C., Ferreira J.J. Digital transformation in the area of health: systematic review of 45 years of evolution. Health and Technology. 2020. Vol. 10. P. 575–586.

209. Marques I.C., Ferreira J.J., Nikitin Y.O., Kul'chyts'kyj O.I. Digital paradigm as a basis for definitions: digital business, digital enterprise, digital transformation. Marketynh i tsyfrovi tekhnolohii. 2019. Vol. 3. No. 4. pp. 77-87. URL: https://journals.indexcopernicus.com/api/file/viewBy$ FileId/907558.pdf

210. Matt C., Hess T., Benlian A. Digital Transformation Strategies. Business & Information Systems Engineering. 2015. Vol. 57, No. 5. P. 339–343.

211. Maturity of telehealth services offered in Europe 2022. Statista. URL: https://www.statista.com/statistics/1421656/maturity-of-telehealth-services-offered-europe/

212. MedCom – Danish Health Data Network. URL: https://medcom.dk/?utm_source=chatgpt.com

213. Medical Device Regulation (MDR). Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.). URL: https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng

214. Medical Devices Act. URL: https://www.riigiteataja.ee/en/akt/524052016001?leiaKehtiv

215. Meskó B., Görög M. A short guide for medical professionals in the era of artificial intelligence. NPJ Digit Med. 2020. Vol. 3. p. 126. URL: https://www.nature.com/articles/s41746-020-00333-z

216. Ministry of Social Affairs of Estonia. URL: https://www.sm.ee/en?utm_source=chatgpt.com

217. Moritz H., Gordian E., Karsten,B. The Data Act Proposal – Literature Review and Critical Analysis - Part I (Art. 1-13, 35) (February 16, 2023). in: Hennemann, M. / Karsten, B. / Wienroeder, M. / Lienemann, G. / Ebner, G. (Eds.). The Data Act Proposal – Literature Review and Critical Analysis. University of Passau Institute for Law of the Digital Society Research Paper S. URL: https://ssrn.com/abstract=4360961

218. National Genome Center. URL: https://www.ngc.dk/?utm_source=chatgpt.com

219. National supervision of EU Artificial Intelligence Act to begin – laws on powers of authorities to take effect at start of the year. Ministry of Economic Affairs and Employment. URL: https://valtioneuvosto.fi/en/-/1410877/national-supervision-of-eu-artificial-intelligence-act-to-begin-laws-on-powers-of-authorities-to-take-effect-at-start-of-the-year?utm_source=chatgpt.com

220. NIS2 Directive implementation in Denmark. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive-denmark?utm_source=chatgpt.com

221. Nordic countries: sharing digital health data 2023. Statista. URL: https://www.statista.com/statistics/1472635/nordic-countries-sharing-digital-health-data/.

222. Novelli C., Hacker Ph., Morley J., Trondal J., Floridi L. A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities. URL: https://arxiv.org/abs/2407.10369

223. Obermeyer Z., Powers B., Vogeli C., Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations. Science. 2019. Vol. 366(6464). Pp. 447-453. URL: https://www.science.org/doi/10.1126/science.aax2342

224. OECD (2022), Health Data Governance for the Digital Age: Implementing the OECD Recommendation on Health Data Governance, OECD Publishing, Paris, DOI: https://doi.org/10.1787/68b60796-en.

225. OECD (2025), “Personal health data systems in OECD countries: Insights into structures and solutions for public access and use”, OECD Health Working Papers, No. 187, OECD Publishing, Paris, DOI: https://doi.org/10.1787/0d118bb0-en.

226. OECD (2025), Health at a Glance 2025: OECD Indicators, OECD Publishing, Paris, DOI: https://doi.org/10.1787/8f9e3f98-en.

227. Olmos Giupponi M.B., Hofmeister H. (Accepted/In press). The regulation of the data economy: The draft EU Data Act – a critical analysis. Zeitschrift für Europarecht, Internationales Privatrecht und Rechtsvergleichung (ZfRV). 2023. Vol. 06. pp. 243-250.

228. Opinion of the European Economic and Social Committee AI, Big Data and rare diseases (exploratory opinion requested by the Danish Presidency of the Council of the EU) (C/2026/24). URL: https://eur-lex.europa.eu/eli/C/2026/24/oj/eng/pdf?utm_source=chatgpt.com

229. Orlando-Salling J. The Digital Services Act in the European periphery: Critical perspectives on EU digital regulation. European Law Open. 2024. Vol. 3(4). pp. 849-864. doi:10.1017/elo.2024.52 https://www.cambridge.org/core/journals/european-law-open/article/digital-services-act-in-the-european-periphery-critical-perspectives-on-eu-digital-regulation/62136D0700099DD3F97630C70E9F0315?utm_source=chatgpt.com

230. Paaso M., Data Privacy Regulation, Compliance Costs and Startup Growth Rates (January 12, 2026). URL: https://ssrn.com/abstract=6535641 or http://dx.doi.org/10.2139/ssrn.6535641

231. Palojoki S., Lehtonen L., Vuokko R. Semantic Interoperability of Electronic Health Records: Systematic Review of Alternative Approaches for Enhancing Patient Information Availability. JMIR Medical Informatics. 2024. Vol. 12. P. e53535-e53535. URL: https://doi.org/10.2196/53535

232. Panch T., Mattie H., Celi L.A. The “inconvenient truth” about AI in healthcare. npj Digit Med. 2019. Vol. 2. P. 77.https://www.nature.com/articles/s41746-019-0155-4

233. Personal Data Protection Act. URL: https://www.riigiteataja.ee/en/akt/507112023002

234. Portuese A. The Digital Markets Act: European Precautionary Antitrust. URL: https://itif.org/publications/2021/05/24/digital-markets-act-european-precautionary-antitrust/?utm_source=chatgpt.com

235. Rak R. Anonymisation, Pseudonymisation and Secure Processing Environments Relating to the Secondary Use of Electronic Health Data in the European Health Data Space (EHDS). European Journal of Risk Regulation. 2024. Vol.15(4). pp. 928-938. doi:10.1017/err.2024.67

236. Rangone N., Megale L. Risks Without Rights? The EU AI Act's Approach to AI in Law and Rule-Making. European Journal of Risk Regulation. 2025. Vol. 16(3). pp.1082-1097. doi:10.1017/err.2025.13

237. Ratwani R.M., Sutton K., Galarraga J.E. Addressing AI algorithmic bias in health care. JAMA. 2024, Vol. 332(13). pp. 1051-1052. URL: https://pubmed.ncbi.nlm.nih.gov/39230911/

238. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj?utm_source=chatgpt.com

239. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1617805554818&uri=CELEX:32017R0745&utm_source=chatgpt.com

240. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj?utm_source=chatgpt.com

241. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2022/1925/oj?utm_source=chatgpt.com

242. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj?utm_source=chatgpt.com

243. Regulation (EU) 2022/868 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). URL: https://eur-lex.europa.eu/legal-content/en/LSU/?uri=CELEX%3A32022R0868&utm_source=chatgpt.com

244. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2023/2854?utm_source=chatgpt.com

245. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. URL: https://eur-lex.europa.eu/eli/reg/2024/1183/oj?utm_source=chatgpt.com

246. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj?utm_source=chatgpt.com

247. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj?uri=CELEX%3A32019R0881&utm_source=chatgpt.com

248. Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng?utm_source=chatgpt.com

249. Richter H. Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing, GRUR International. 2023. Vol. 72, Is. 5. pp. 458-470. URL: https://doi.org/10.1093/grurint/ikad014

250. Riigi Infosüsteemi Amet. URL: https://www.ria.ee/

251. Riigi teataja. URL: https://www.riigiteataja.ee/en?utm_source=chatgpt.com

252. Sałek K., Fajdek P. Analysis of the implementation of the NIS2 directive in the Weimar Triangle countries. Central European Review of Economics & Finance. 2025. Vol. 50(1). Pp. 41-52.DOI: https://doi.org/10.24136/ceref.2025.003

253. Schmitz-Berndt S. Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. Journal of Cybersecurity. 2023. Vol. 9. I. 1, tyad009. URL: https://doi.org/10.1093/cybsec/tyad009

254. Sendak M.P., D'Arcy J., Kashyap S., et al. A path for translation of machine learning products into healthcare delivery. EMJ Innov. 2020. URL: https://www.emjreviews.com/innovations/article/a-path-for-translation-of-machine-learning-products-into-healthcare-delivery/

255. Services til sundhedssektoren. URL: https://sundhedsdatastyrelsen.dk/cybersikkerhed/services-til-sundhedssektoren?utm_source=chatgpt.com

256. Smit, JA.R., Mostert, M., van der Graaf, R. et al. Specific measures for data-intensive health research without consent: a systematic review of soft law instruments and academic literature. Eur J Hum Genet. 2024. Vol.32. pp. 21–30. DOI: https://doi.org/10.1038/s41431-023-01471-0

257. Sousa e Silva, Nuno, The Artificial Intelligence Act: Critical Overview (July 30, 2024). URL: https://ssrn.com/abstract=4937150 or http://dx.doi.org/10.2139/ssrn.4937150

258. Styrelsen for Samfundssikkerhed. URL: cfcs.dk/?utm_source=chatgpt.com

259. Sundhed.dk – the Danish eHealth Portal. URL: https://www.sundhed.dk/?utm_source=chatgpt.com

260. Sundhedsdata-styrelsen. Danish Health Data Authority https://sundhedsdatastyrelsen.dk/?utm_source=chatgpt.com

261. Telehealth use and policies in Europe 2022. Statista. URL: https://www.statista.com/statistics/1421332/telehealth-use-and-policies-in-europe/

262. Tervisekassa. Estonian Health Insurance Fund. URL: https://tervisekassa.ee/

263. The 2026 Digital Decade eHealth Indicator Study. URL: https://digital-strategy.ec.europa.eu/en/library/2026-digital-decade-ehealth-indicator-study?utm_source=chatgpt.com

264. The Digital Economy and Society Index (DESI). Shaping Europe’s digital future. URL: https://digital-strategy.ec.europa.eu/en/policies/desi.

265. The EU MDR (Regulation (EU) 2017/745) covers medical device regulation and approval throughout the EU. URL: https://www.tuvsud.com/en/industries/medical-devices/medical-device-regulation

266. Topol E.J.. High-performance medicine: the convergence of human and artificial intelligence. Nat Med. 2019. Vol. 25(1). pp. 44-56. URL: https://www.nature.com/articles/s41591-018-0300-7

267. Vastaamo board fires CEO, says he kept data breach secret for year and a half. URL: https://yle.fi/a/3-11614603?utm_source=chatgpt.com

268. Verghese A., Shah N.H., Harrington R.A. What this computer needs is a physician: humanism and artificial intelligence. JAMA. 2018. Vol. 319(1). Pp.19-20. URL: https://pubmed.ncbi.nlm.nih.gov/29261830/

269. Vial G. Understanding Digital Transformation: A Review and a Research Agenda. The Journal of Strategic Information Systems. 2019. Vol. 28, No. 2. P. 118–144.

270. Vogel V., Ziegler N. Kritikalität: Von der BSI-KritisV zur NIS2-Richtlinie. International Cybersecurity Law Review. 2023. Vol. 4. pp. 1–19. URL: https://link.springer.com/article/10.1365/s43439-022-00077-4?utm_source=chatgpt.com

271. Vogeser M., Brüggemann M., Lennerz J., Stenzinger A., Gassner Ulrich M., Partial Postponement of the Application of the In Vitro Diagnostic Medical Devices Regulation in the European Union. Clinical Chemistry, 2022. Vol. 68, I.6, pp. 856–857. URL: https://doi.org/10.1093/clinchem/hvac048

272. Vogeser M., Brüggemann M., Lennerz J., Stenzinger A., Gassner Ulrich M. Laboratory-Developed Tests in the New European Union 2017/746 Regulation: Opportunities and Risks. Clinical Chemistry. 2022. Vol. 68, I 1, Pp. 40–42. DOI: https://doi.org/10.1093/clinchem/hvab215

273. Vokinger K.N., Feuerriegel S., Kesselheim A.S. Continual learning in medical devices: FDA's action plan and beyond. Lancet Digit Health. 2021. Vol. 3(6).e337-e338. URL: https://www.thelancet.com/journals/landig/article/PIIS2589-7500(21)00076-5/fulltext

274. von Ditfurth L., Lienemann G. The Data Governance Act: – Promoting or Restricting Data Intermediaries? Competition and Regulation in Network Industries. 2022. Vol. 23(4). pp. 270-295.

275. Westerman G., Bonnet D., McAfee A. Leading Digital: Turning Technology into Business Transformation. Harvard Business Press, 2014. 292 p.

276. Westerman G., Bonnet D., McAfee A. The Nine Elements of Digital Transformation. MIT Sloan Management Review. 2014. Vol. 55, No. 3. P. 1–6.

277. White Paper on AI, 2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0065

278. Wiewiórowski W. Digital Health 2020 - EU on the Move. URL: https://www.edps.europa.eu/data-protection/our-work/publications/speeches-articles/digital-health-2020-eu-move-wojciech_fr

279. World Bank Data360. URL: https://data360.worldbank.org/en/indicator/UN_EGDI_EGDI?view=bar

280. World Health Organization. Global Strategy on Digital Health 2020–2025. Geneva: WHO, 2021.

281. World Health Organization. Global Strategy on Digital Health 2020–2025. Geneva: WHO, 2021. URL: https://www.who.int/publications/i/item/9789240020924

282. Yao X., Sun Zh., Man H. Balancing Scientific and Commercial Interests: The European Health Data Space Response to Commercial Scientific Research. URL: https://journals.sagepub.com/doi/10.1177/00469580261420714?utm_source=chatgpt.com