

DOI 10.34132/pard2026.32.10

Отримано: 12 травня 2025

Змінено: 27 вересня 2025

Прийнято: 08 січня 2026

Опубліковано:

29 травня 2026

Received: 12 May 2025

Revised: 27 September 2025

Accepted: 08 January 2026

Published:

29 May 2026

Kostiantyn Naumenko

PUBLIC GOVERNANCE OF THE HIDDEN RISKS OF DIGITAL TRANSFORMATION IN THE HEALTHCARE SYSTEM

The article states that the digital transformation of the healthcare system creates new opportunities for improving the accessibility, quality, transparency, and continuity of medical service delivery; however, it simultaneously generates a complex set of risks that are not always evident at the stage of implementing digital technologies. The hidden risks of healthcare digitalization are examined, and the need for their preventive, comprehensive, and coordinated management at the level of public policy is substantiated. It is emphasized that, unlike explicit threats, hidden risks may remain unnoticed at the initial stage of digital technology implementation and may manifest themselves unexpectedly. Particular attention is paid to the phenomenon of a «digital pandemic», the cascading nature of which is reflected in its ability to cause chain disruptions in the functioning of electronic health records, registries, medical information systems, telemedicine services, laboratory platforms, electronic prescriptions, referrals, financing systems, and managerial analytics. It is underlined that the danger of a «digital pandemic» in the context of the development of space-digital infrastructure lies not only in the speed at which digital disruptions spread, but also in their ability to simultaneously affect different levels of the healthcare system. It is emphasized that public risk management related to a «digital pandemic» should be aimed not only at responding after an incident has occurred, but primarily at preventing the cascading spread of threats. It is noted that this

requires an integrated digital infrastructure, interoperability standards, data backup mechanisms, independent auditing of digital solutions, a clear distribution of responsibility among healthcare system actors, and personnel training for actions in the event of digital failures. Practical recommendations for public management of the hidden risks associated with the digital transformation of the healthcare system are developed. It is substantiated that the implementation of the proposed recommendations will make it possible to minimize the consequences of a potential «digital pandemic», preserve the trust of patients and healthcare professionals in digital technologies, and ensure the sustainability of the digital transformation of the healthcare system.

Key words: *hidden risks of digitalization, healthcare system, public governance of digitalization risks, digital pandemic, orbital-digital vulnerability of the healthcare system, orbital-digital resilience of the healthcare system, digital quarantine.*

Постановка проблеми у загальному вигляді. Сучасна система охорони здоров'я дедалі менше функціонує як сукупність окремих медичних закладів, адміністративних процедур і професійних рішень лікаря. Унаслідок цифрової трансформації вона поступово перетворюється на складну соціотехнічну систему, у якій медична допомога, управлінські рішення, фінансування, обіг лікарських засобів, маршрутизація пацієнтів і комунікація між учасниками процесу залежать від цифрових платформ, реєстрів, каналів зв'язку, електронної ідентифікації та доступу до даних. Тому предметом державного управління у сфері охорони здоров'я стає вже не лише організація медичних послуг, а й забезпечення надійності цифрового середовища, у межах якого ці послуги створюються, координуються та надаються.

Ця зміна є принциповою, оскільки цифровізація не просто прискорює наявні управлінські процеси, а змінює саму природу залежностей усередині системи охорони здоров'я. Якщо раніше збій в окремому адміністративному або технічному процесі міг мати переважно локальні наслідки, то в цифровій системі порушення

доступу до реєстру, електронного медичного запису, електронного рецепта, телекомунікаційного каналу чи хмарної інфраструктури здатне вплинути одразу на багато учасників – пацієнтів, лікарів, аптечні заклади, лабораторії, управлінські органи та фінансові механізми. Саме тому в Глобальній стратегії ВООЗ [1] наголошено, що цифрова трансформація системи охорони здоров'я потребує не лише впровадження нових сервісів, а й зміни акцентів та переосмислення державного управління ризиками, які виникають унаслідок зростання цифрової залежності медичного сектору. Це означає, що цифрова трансформація системи охорони здоров'я не може бути зведена лише до технічної модернізації, вона має передбачати управлінську відповідальність за дані, інфраструктуру, безпеку, справедливий доступ і сталість цифрових рішень.

Тож, експерти Міжнародного союзу електрозв'язку (International Telecommunication Union, ITU), Управлінням ООН зі зменшення ризику стихійних лих (United Nations Office for Disaster Risk Reduction, UNDRR) та Інституту політичних досліджень Парижа (Institut d'études politiques de Paris, Scie Sciences Po), закликають уряди держав до скоординованих дій з управління прихованими ризиками цифрової трансформації [2], спрямованих на підвищення цифрової стійкості та захист системи охорони здоров'я, що саме і підкреслює актуальність даного дослідження.

Аналіз останніх досліджень і публікацій. Проблематика цифрової трансформації системи охорони здоров'я активно досліджується як у зарубіжній, так і у вітчизняній науковій літературі. У більшості зарубіжних праць даний процес розглядається як чинник підвищення доступності медичних послуг, оптимізації управлінських процесів, розвитку електронних медичних записів, аналітики даних, штучного інтелекту та пацієнтоорієнтованих сервісів. Втім, Дж. Карнісеро та П. Серра у праці [3] пропонують розглядати цифрову трансформацію не лише як технологічний процес, а як зміну схем управління системою охорони здоров'я, що потребує відповідних інституційних, нормативних і організаційних механізмів. Схожої

позиції дотримуються Р. Тертуліно, Н. Антунес та Х. Мораїс, які наголошують що розвиток інтероперабельності електронних медичних записів має супроводжуватися належним управлінням ризиками безпеки, приватності та захисту медичних даних [4]. А. Гарсія-Перес та ін. пов'язують ризики цифровізації охорони здоров'я з необхідністю управління цифровою стійкістю медичних систем як умови їхньої безпечної та безперервної роботи [5]. П. Ево та Т. Вартіайнен, доводить, що ризики цифрової медицини мають не лише технічну, а й організаційну, кадрову та соціотехнічну природу [6]. Е. Лі та співавтори показують, що інтероперабельність електронних медичних записів є не лише технічним питанням, а важливим чинником безпеки пацієнтів [7]. Н. Бесіл та співавтори аналізують ризики безпеки баз даних електронних медичних записів, зокрема можливість витоку медичних даних, несанкціонованого доступу та доводять потребу у впровадженні належних захисних механізмів [8].

В українській науковій літературі цифрова трансформація охорони здоров'я здебільшого досліджується через призму впровадження eHealth, електронних медичних записів, телемедицини, електронних сервісів, цифрового управління закладами охорони здоров'я та нормативно-правового забезпечення цифровізації. Так, Н. Слободян та Н. Панчишин серед викликів eHealth виокремлює кібербезпеку, електронні медичні записи та ризики цифровізації медицини [9]. В. Якобчук та ін. пов'язує ризики цифровізації з кібербезпекою, телемедициною, цифровими компетентностями та публічним управлінням в умовах війни. Є. Кобрусєва акцентує увагу на інформаційній безпеці медичної сфери в період правового режиму воєнного стану, зокрема на питаннях обміну та захисту медичної інформації [10].

Отже, проведений аналіз свідчить, що цифровізація системи охорони здоров'я розглядається в науковій літературі переважно через призму її переваг, технічних викликів, питань кібербезпеки та захисту інформації. Втім, потенційні приховані ризики цифрової трансформації, зумовлені прискореним розвитком космічно-цифрової інфраструктури

на низькій навколоземній орбіті, у складі супутникових угруповань або в навколomisячному просторі, залишаються недостатньо дослідженими. Особливої уваги потребують їхній каскадний характер, можливість поширення вразливостей між взаємопов'язаними інфраструктурними компонентами, а також механізми державного управління такими ризиками, що саме і визначає актуальність та практичну значимість даного дослідження.

Формулювання мети статті (постановка завдання).

Метою статті є дослідження особливостей державного управління ризиками цифровізації системи охорони здоров'я в умовах зростання її залежності від космічно-цифрової інфраструктури та обґрунтування превентивних інструментів, здатних забезпечити своєчасне виявлення прихованих загроз, зменшення їх каскадного впливу й підтримання стійкого функціонування цифрової медицини.

Виклад основного матеріалу дослідження. Цифрова трансформація системи охорони здоров'я сьогодні є не лише технологічним, а й управлінським, соціальним та безпековим процесом. Її значення виходить далеко за межі впровадження електронних сервісів, оскільки цифрові рішення поступово змінюють саму логіку організації медичної допомоги, обігу медичних даних, взаємодії між пацієнтом, лікарем, закладом охорони здоров'я та державою [16;17]. У глобальному вимірі цей процес розглядається як один із ключових інструментів зміцнення систем охорони здоров'я. Зокрема, Всесвітня організація охорони здоров'я у Global Strategy on Digital Health 2020–2027 наголошує, що цифрові ініціативи мають реалізовуватися на основі цілісної стратегії, яка поєднуватиме фінансові, організаційні, людські й технологічні ресурси [1].

Водночас саме така глибока інтеграція цифрових технологій у сферу охорони здоров'я породжує нову управлінську дилему. З одного боку, електронні медичні записи, електронні рецепти, телемедицина, цифрові реєстри, аналітика даних, штучний інтелект і платформи

обміну інформацією підвищують доступність, прозорість та ефективність медичних послуг. З іншого боку, що більшою стає залежність системи охорони здоров'я від цифрової інфраструктури, то менш очевидними, але потенційно масштабнішими стають ризики її порушення[15]. Через це питання цифрової трансформації системи охорони здоров'я не може обмежуватися лише оцінкою кількості впроваджених сервісів або рівня автоматизації процесів. Воно потребує аналізу того, наскільки система здатна безпечно функціонувати.

Особливої гостроти це питання набуває з прискореним розвитком космічно-цифрової інфраструктури, активне масштабування якої пов'язано зі зростанням глобального попиту на обчислювальні потужності, розвитком штучного інтелекту, енергетичними обмеженнями наземних дата-центрів і прагненням використовувати переваги космічного середовища. Зокрема, у 2025 р. Lonestar Data Holdings публічно заявив про створення космічно-цифрової інфраструктури зі зберігання даних у низькій навколоземній орбіті та на Місяці. Мова йде про запуск фізичного місячного дата-центру Freedom Data Center, інтегрованого до посадкового модуля Athena компанії Intuitive Machines, доставку якого було здійснено ракетою SpaceX Falcon 9, а також про успішне тестування зберігання даних у місячному та диспунарному просторі [11]. Google, у межах Project Suncatcher, також завершує створення масштабованої космічної AI-інфраструктури на основі супутникових угруповань із TPU-чипами та оптичними каналами зв'язку, і планує запуск двох прототипів супутників до початку 2027 року, які протестують обладнання на орбіті, закладаючи основу для майбутньої ери масово масштабованих обчислень у космосі [12]. За проєктом ASCEND, що фінансується ЄС, також передбачено встановлення на орбіті великих модульних космічних інфраструктур з роботизованим складанням, космічною сонячною енергією потужністю мегават, високошвидкісним оптичним зв'язком, недорогими та багаторазовими пусковими установками [13].

За оцінками експертів OECD, значна частина критичної інфраструктури вже наразі функціонує із залученням космічно-

цифрових технологій, зокрема у сферах транспорту, логістики та стратегічних комунікацій. Система охорони здоров'я також поступово набуває залежності від таких технологій, оскільки безперервність надання медичних послуг дедалі більше визначається стабільністю цифрових платформ, каналів зв'язку, навігаційних і супутникових сервісів [14]. Саме тому в умовах розвитку космічно-цифрової інфраструктури державне управління цифровою трансформацією системи охорони здоров'я має охоплювати не лише очевидні ризики eHealth, а й приховані ризики цифровізації системи надання медичної допомоги. До їх числа вважаємо слід віднести такі (рис.1).

Всі перелічені групи ризиків не існують ізольовано. Їхня головна небезпека полягає в можливості каскадного поєднання. В Звіті ITU, UNDRR та Sciences Po [2] наголошується, що критичні цифрові порушення здатні миттєво поширюватися між секторами й кордонами, створюючи каскадний ефект, тобто так звану «cyber pandemic» (цифрову пандемію).

Супутниково-комунікаційні ризики	Ризики, пов'язані із залежністю охорони здоров'я від супутникового зв'язку та супутникового інтернету (зокрема, збій зв'язку), що потребують резервування, тестування та кризових сценаріїв
Навігаційно-часові ризики	Ризики, пов'язані із залежністю від глобальних навігаційних супутникових систем — GPS, Galileo, GLONASS, та ін. систем позиціонування, навігації (GPS/GNSS-спуфінг або глушіння)
Ризики космічної погоди	Ризики, пов'язані з впливом сонячних бур, геомагнітних збурень та інших явищ на супутники, GNSS, радіозв'язок, авіацію, енергомережі й цифрову інфраструктуру
Орбітально-Big Data ризики	Ризики залежності від провайдерів, розміщенням дата-центрів, обчислювальних потужностей і AI-інфраструктури в космосі, складності технічного обслуговування тощо
Орбітально-сміттєві ризики	Ризики, пов'язані зі зростанням кількості супутників, уламків, фрагментаційних подій і потенційної деградації орбітального середовища
Геоекономічні космічні ризики	Ризики, пов'язані з розвитком космічної економіки, яка дедалі більше масштабується через приватних і транснаціональних операторів

Рис. 1. Приховані ризики цифрової трансформації системи охорони здоров'я в умовах прискореного розвитку космічно-цифрової інфраструктури
Джерело: складено автором

В даному випадку мова йде не про «кіберпандемію» і не про сценарії масованої кібератаки. Йдеться про ширше явище – можливий каскадний збій критичних космічно-цифрових систем, коли порушення в одній ланці космічної цифрової інфраструктури здатне швидко вплинути на інші сектори та сервіси.

На сторінці звіту ITU/ WTISD 2026 сценарій «cyber pandemic» пояснюється як можливість виникнення ситуації, за якої перестають працювати мобільний зв'язок та інтернет, не проходять платежі, лікарні втрачають доступ до даних пацієнтів, а системи екстреного оповіщення не спрацьовують [2]. З огляду на це предметом державного управління прихованими ризиками цифрової трансформації стає не лише захист від зловмисних дій, а й забезпечення космічно-цифрової стійкості системи охорони здоров'я. А отже, державне управління має бути спрямоване не лише на подолання наслідків цифрових інцидентів після їх виникнення, а насамперед на запобігання їх каскадному поширенню. Такий підхід потребує переходу від традиційного реактивного реагування до превентивного управління прихованими ризиками цифрової трансформації – новітнього напрямку державного управління, орієнтованого на забезпечення в умовах прискореного розвитку космічно-цифрової інфраструктури, орбітально-цифрової стійкості системи охорони здоров'я.

Відповідно до Global strategy on digital health 2020-2027 [1] превентивне управління має бути спрямоване на раннє виявлення, прогнозування, запобігання та мінімізацію космічно-цифрових загроз системі охорони здоров'я, які внаслідок потенційного каскадного поширення здатні порушити безперервність надання медичних послуг, безпеку персональних даних, стабільність медичної логістики, роботу екстреної допомоги та довіру громадян до цифрової медицини. [1]. А отже, на нашу думку, воно має включати наступні блоки (рис. 2):

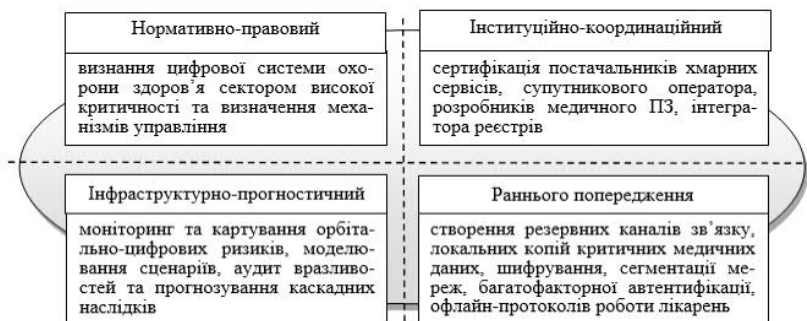


Рис. 2. Схематичне зображення цілісної архітектури механізму державного управління прихованими ризиками цифрової трансформації системи охорони здоров'я в умовах прискореного розвитку космічно-цифрової інфраструктури.

Джерело: складено автором

При цьому до кожного з блоків мають увійти інструменти державного управління, спрямовані на зниження космічно-цифрової вразливості системи охорони здоров'я, яка з посиленням залежності цифрових медичних сервісів від супутникових, навігаційних, телекомунікаційних і хмарних компонентів, невідомо зростає (рис. 3).

Виходячи з рекомендованого до застосування інструментарію державного управління прихованими ризиками цифрової трансформації системи охорони здоров'я, уряду України слід вжити сукупність заходів наднаціонального, національного та територіального регуляторного характеру. При цьому на національному рівні для забезпечення дієвості механізмів превентивного управління прихованими ризиками цифрової трансформації системи охорони здоров'я необхідно сформулювати систему міждержавної координації у сфері космічно-цифрової безпеки. Це дозволить державам не лише реагувати на інциденти, а й завчасно попереджати їх поширення.

В той же час, для забезпечення дієвості механізмів превентивного управління прихованими ризиками цифрової трансформації системи охорони здоров'я на національному рівні необхідно

сформувати цілісну управлінську систему, яка поєднуватиме правове регулювання, інституційну відповідальність, фінансове забезпечення, технічні стандарти та постійний моніторинг ризиків. Йдеться не лише про ухвалення окремих нормативних актів, а про створення єдиної державної політики щодо управління космічно-цифровими загрозами.



Рис. 3. Інструментарій державного управління прихованими ризиками цифрової трансформації системи охорони здоров'я в умовах прискореного розвитку космічно-цифрової інфраструктури.

Джерело: сформовано автором

Окрему увагу слід приділити запровадженню обов'язкових процедур виявлення та оцінювання космічно-цифрової залежності медичних сервісів. Для цього доцільно створити державний реєстр критичних цифрових медичних систем, визначити їхню залежність від хмарних платформ, супутникового зв'язку, GNSS-навігації, телемедицини, зовнішніх цифрових сервісів і постачальників технологічних рішень. Такий підхід дозволить заздалегідь встановити найбільш уразливі елементи системи охорони здоров'я та передбачити заходи їх резервування.

Однак реальна стійкість медичної інфраструктури формується не лише через нормативне закріплення правил, а й через їх практичне застосування у конкретних територіальних умовах. Саме тому логічним продовженням національних заходів є перехід до територіального рівня, де загальнодержавні підходи мають бути адаптовані до реальних умов функціонування регіональних медичних мереж, наявних ресурсів, цифрової інфраструктури та локальних вразливостей.

Відтак, під державним управлінням прихованими ризиками цифровізації системи охорони здоров'я варто розуміти цілісну систему випереджального регулювання, спрямовану на збереження цифрової стійкості, безперервності медичної допомоги та захист персональних даних. Його практичне значення полягає у необхідності формування нової моделі державного управління процесом цифровізації сектору охорони здоров'я, здатної своєчасно виявляти приховані загрози цифровізації, оцінювати їх міжсекторальні та каскадні наслідки, запобігати цифровим збоям і забезпечувати надійне надання медичної допомоги в умовах прискореного розвитку космічно-цифрової інфраструктури.

Висновки. Таким чином, за результатами дослідження обґрунтовано, що цифрова трансформація системи охорони здоров'я, поряд із очевидними перевагами щодо підвищення доступності, якості, прозорості та безперервності медичних послуг, формує комплекс прихованих ризиків, які потребують цілеспрямованого державного управління. Встановлено, що такі ризики можуть залишатися непомітними на початкових етапах упровадження цифрових технологій, однак згодом здатні проявлятися у вигляді збоїв.

Доведено, що особливо небезпечним проявом прихованих ризиків цифровізації охорони здоров'я є феномен «цифрової пандемії», який має каскадний характер впливу. Його сутність полягає в тому, що локальна цифрова проблема, кібератака або збій окремого сервісу можуть спричинити ланцюгові порушення в роботі електронних медичних записів, реєстрів, медичних інформаційних систем, телемедичних платформ, лабораторних

сервісів, електронних рецептів, направлень, фінансових механізмів та управлінської аналітики.

Запропоновано практичні рекомендації щодо вдосконалення державного управління прихованими ризиками цифрової трансформації системи охорони здоров'я. Їх реалізація сприятиме мінімізації наслідків потенційної “цифрової пандемії”, посиленню кіберстійкості медичної цифрової інфраструктури, захисту персональних медичних даних, забезпеченню безперервності надання медичних послуг, збереженню довіри пацієнтів і медичних працівників до електронних сервісів та сталості цифрової трансформації медичної сфери.

Перспективами подальших досліджень є моделювання сценаріїв каскадного поширення цифрових загроз, а також формування інструментів моніторингу цифрової стійкості системи охорони здоров'я.

ДЕРЖАВНЕ УПРАВЛІННЯ ПРИХОВАНИМИ РИЗИКАМИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я

У статті констатовано, що цифрова трансформація системи охорони здоров'я створює нові можливості для підвищення доступності, якості, прозорості та безперервності надання медичних послуг, однак водночас формує комплекс ризиків, які не завжди є очевидними на етапі впровадження цифрових технологій. Досліджено приховані ризики цифровізації системи охорони здоров'я та аргументовано необхідність їх превентивного, комплексного й координованого управління на рівні державної політики. Акцентовано, що на відміну від відкритих загроз, приховані ризики можуть залишатися непомітними на початковому етапі впровадження цифрових технологій та проявлятися неочікувано. Особливу увагу приділено феномену «цифрової пандемії», каскадний характер поширення якої проявляється у здатності спричиняти ланцюгові порушення в роботі електронних медичних записів, реєстрів, медичних інформаційних систем, телемедичних сервісів, лабораторних

платформ, електронних рецептів, направлень, систем фінансування та управлінської аналітики. Підкреслено, що небезпека «цифрової пандемії» в умовах розвитку космічно-цифрової інфраструктури полягає не лише у швидкості поширення цифрових порушень, а й у їх здатності одночасно впливати на різні рівні системи охорони здоров'я. Наголошено, що державне управління ризиками «цифрової пандемії» має бути спрямоване не лише на реагування після виникнення інциденту, а насамперед на попередження каскадного поширення загроз. Зазначено, що для цього необхідні цілісна цифрова інфраструктура, стандарти інтероперабельності, резервування даних, незалежний аудит цифрових рішень, чіткий розподіл відповідальності між суб'єктами системи охорони здоров'я та підготовка персоналу до дій у разі цифрових збоїв. Розроблено практичні рекомендації з державного управління прихованими ризиками цифрової трансформації системи охорони здоров'я. Обґрунтовано, що впровадження поданих пропозицій дозволить мінімізувати наслідки потенційної «цифрової пандемії», зберегти довіру пацієнтів і медичних працівників до цифрових технологій та забезпечити сталість цифрової трансформації системи охорони здоров'я.

Ключові слова: приховані ризики цифровізації, система охорони здоров'я, державне управління ризиками цифровізації, цифрова пандемія, орбітально-цифрова вразливість системи охорони здоров'я, орбітально-цифрова стійкість системи охорони здоров'я, цифровий карантин.

Author Contributions: Conceptualization, K.N.; Writing – original draft, K.N.; Writing – review & editing, K.N.. Author has read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable as study did not include human subjects.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Global strategy on digital health 2020-2027. (2025). *iris.who.int*. Retrieved from: <https://iris.who.int/server/api/core/bitstreams/a64d584f-015b-471f-9d86-9ea263cfb516/content> [in English].
2. When digital systems fail: An expert report. (n.d.). (2026). *www.itu.int*. Retrieved from: <https://www.itu.int/pub/S-REP-WTISD-2026> [in English].
3. Carnicero, J., & Serra, P. (2020). *Governance for Digital Health: The Art of Health Systems Transformation*. Retrieved from: <https://doi.org/10.18235/0002661> [in English].
4. Tertulino, R., Antunes, N. & Morais, H. (2024). Privacy in electronic health records: a systematic mapping study. *J Public Health (Berl.)*, (Vol. 32), (pp. 435-454). Retrieved from: <https://doi.org/10.1007/s10389-022-01795-z> [in English].
5. Garcia-Perez, A., Gabriel Cegarra-Navarro, J., Sallos, M., Martinez-Caro, E., & Chinnaswamy, A. (2023). Resilience in healthcare systems: Cyber security and digital transformation. *Technovation*, (Vol. 121). Retrieved from: <https://doi.org/10.1016/j.technovation.2022.102583> [in English].
6. Ewoh, P., & Vartiainen, T. (2024). Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review. *J Med Internet Res*, (Vol. 24). Retrieved from: <https://doi.org/10.2196/46904> [in English].
7. Li, E., Clarke, J., & Neves, A.L. (et al.). (2021). Electronic Health Records, Interoperability and Patient Safety in Health Systems of High-income Countries: A Systematic Review Protocol. *BMJ Open*, (Vol. 11). Retrieved from: <https://doi.org/10.1136/bmjopen-2020-044941> [in English].
8. Basil, N., Ambe, S., Ekhator, C., & Fonkem, E. (2022). Health Records Database and Inherent Security Concerns: A Review of the Literature. *Cureus*, 14(10). Retrieved from: <https://doi.org/10.7759/cureus.30168> [in English].
9. Slobodian, N.O., Panchyshyn, N.Ya., Kondratiuk, V.V., Lytvynova, O.N., & Petrashyk, Yu.M. (2025). Vprovadzhennia elektronnykh medychnykh zapysiv: perevahy, vyklyky ta rol v upravlinni zakladamy okhorony zdorovia [Implementation of electronic medical records: advantages, challenges and role in healthcare management institutions]. *Visnyk sotsialnoi hihiieny ta orhanizatsii okhorony zdorovia Ukrainy – Bulletin of social hygiene and health-care organization of Ukraine*, 1(103), (pp. 46-51). Retrieved from: <https://doi.org/10.11603/1681-2786.2025.1.15342> [in Ukrainian].
10. Yakobchuk, V.P., Ivaniuk, O.V., & Krut, V.V. (2024). Upravlinnia informatsiinymy tekhnolohiyamy v sferi okhorony zdorovia v umovakh

voiennoho stanu [Management of information technologies in the healthcare sector under martial law]. *Ekonomichnyi prostir – Economic Space*, 195, (pp. 193-200). Retrieved from: <https://doi.org/10.30838/EP.195.193-200> [in Ukrainian].

11. Starvault: the Future of Data storage is in Space. (n.d.). (2025). *www.lonestar.space*. Retrieved from: https://www.lonestar.space/?utm_source=chatgpt.com [in English].

12. Beals, T. (2025). Exploring a space-based, scalable AI infrastructure system design. *research.google*. Retrieved from: https://research.google/blog/exploring-a-space-based-scalable-ai-infrastructure-system-design/?utm_source=chatgpt.com [in English].

13. Advanced Space Cloud for European Net zero emissions and Data sovereignty. (n.d.). (2022). *cordis.europa.eu*. Retrieved from: https://cordis.europa.eu/project/id/101082517?utm_source=chatgpt.com [in English].

14. Kobrusieva, Ye.A. (2025). Informatsiina bezpeka u medychnii sferi u period pravovoho rezhymu voiennoho stanu [Information security in the medical sphere during the period of the legal regime of martial law]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho universytetu. Serii: Pravo – Scientific Bulletin of Uzhhorod National University. Series: Law*, 90, (P. 3), (pp. 220-225). Retrieved from: <https://doi.org/10.24144/2307-3322.2025.90.3.31> [in Ukrainian].

15. Bielai, S., Antonova, L., Hololobov, S., Yevtushenko, I., & Sporyshev, K. (2024). The impact of a practice-oriented paradigm on public administration and national security. *International Journal of Sustainable Development and Planning*, (Vol. 19), 1, (pp. 277-288). Retrieved from: <https://doi.org/10.18280/ijstdp.190126> [in English].

16. Budniuk, O., Pereviznyk, V., Mazurenko, H., Shcherbakov, S., & Antonova, L. (2022). Digitalization as a Means of Anti-Corruption Policy in the Sphere of Health Care in Ukraine. *International Journal of Computer Science and Network Security*, (Vol. 22), 7, (pp. 320-326). Retrieved from: <https://doi.org/10.22937/IJCSNS.2022.22.7.39> [in English].

17. Havrychenko, D., Antonova, L., Petryk, S., Avtomieienko, Y., Tyshko, D., & Samchuk, P. (2023). Economic assessment of regional challenges of the healthcare sector of Ukraine in the context of sustainable development. *Financial and Credit Activity Problems of Theory and Practice*, 1(48), (pp. 409-417). Retrieved from: <https://doi.org/10.55643/fcaptop.1.48.2023.3948> [in English].

Відомості про автора / Information about the Author

Костянтин Науменко, керівник ендоскопічного напрямку ТОВ «Медичний дім «Odrex», м. Одеса, Україна. E-mail: naumenko.kos@gmail.com, orcid: <https://orcid.org/0000-0002-0252-3118>.

Kostiantyn Naumenko, head of Endoscopic Department, Odrex Medical Home LLC, Odessa, Ukraine. E-mail: naumenko.kos@gmail.com, orcid: <https://orcid.org/0000-0002-0252-3118>.

Naumenko, K. (2026). Public governance of the hidden risks of digital transformation in the healthcare system. *Public Administration and Regional Development*, 32, 636-651. <https://doi.org/10.34132/pard2026.32.10>